COMITÉ DE COMPRAS

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO

BASES DE LA LICITACIÓN PÚBLICA ESTATAL N° 5627D301-002-2024

SERVICIOS INTEGRALES DE INFRAESTRUCTURA DE CÓMPUTO

NO SE ACEPTA LA PRESENTACIÓN DE PROPUESTAS EN FORMA ELECTRÓNICA O POR MENSAJERÍA.

VILLAHERMOSA, TABASCO, 20 DE MARZO 2024

CONTENIDO

5. DOCUMENTOS DE GARANTÍA

5.1. Garantía de seriedad de la propuesta económica (cheque)
5.2. Garantía de cumplimiento (fianza)
5.3. Ejecución de garantías

6. CONTRATO

6.1. Generalidades
6.2. Penas convencionales
6.3. Devoluciones al proveedor
6.4. Cantidades adicionales y ampliación de vigencia por modificaciones a los contratos
6.5. Rescisión y suspensión
6.6. De la inhabilitación del (los) Licitante (s)
6.7. De las inconformidades y controversias

A N E X O S

ANEXO 1. Acreditamiento de la personalidad

ANEXO 2. Aceptación de términos de las bases

ANEXO 3. Manifestación de no encontrarse en alguno de los supuestos del artículo 51 de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco

ANEXO 4. Declaración de Integridad (artículo 35, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco)

ANEXO 5. Especificaciones técnicas de los servicios que se requieren

ANEXO 6. Cumplimiento en cantidades y características de los Servicios Integrales De Infraestructura De Cómputo (artículo 53 de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco)

ANEXO 7. Formato de oferta económica

ANEXO 8. Declaraciones sobre la garantía de cumplimiento (Fianza)

ANEXO 9. Calendario de actos

ANEXO 10. Formato para la presentación de preguntas a la Convocante

1. REFERENCIAS DE LA LICITACIÓN

1.1. Marco jurídico

La presente Licitación se lleva a cabo con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 76 párrafos décimo tercero, décimo cuarto y décimo quinto de la Constitución Política del Estado Libre y Soberano de Tabasco; 21 párrafo primero, 22 fracción I, 24 fracción I, 26, 27, 28, 29, 30, 31, 32, 33, 34, 41 y 42 de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco; 1, 4, 7, 8, 13, 19, 19 Bis, 21 Bis último párrafo, 29, 32, 34, 35, 36, 37, 37 Bis, 38 y 39 del Reglamento de la Ley Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco.

Por lo anterior, el Comité de Compras del Instituto Electoral y de Participación Ciudadana de Tabasco, convoca a todas aquellas personas físicas y jurídicas colectivas legalmente constituidas, interesadas en participar en la presente Licitación, siempre y cuando satisfagan los requisitos de la convocatoria y las presentes bases, con la finalidad de asegurar a la Convocante las mejores condiciones en cuanto a economía, eficiencia, imparcialidad, honradez , por lo tanto, los interesados en participar deberán sujetarse a las siguientes:

B A S E S

1.2. Glosario de términos

Para los fines de la presente Licitación, en lo sucesivo se denominará:

Comité:	El Comité de Compras del Instituto Electoral y de Participación Ciudadana de Tabasco.
Contraloría:	La Contraloría General del Instituto Electoral y de Participación Ciudadana de Tabasco.
Contrato:	El Acto jurídico bilateral y formal que se constituye por el acuerdo de voluntades que se establece entre la Convocante y el (los) proveedor (es) adjudicados en la presente

licitación.

Convocante:	El Instituto Electoral y de Participación Ciudadana de Tabasco.
Ley:	La Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco.
Licitantes:	Personas físicas y jurídicas colectivas inscritas y vigentes en el Directorio de Proveedores del Instituto Electoral y de Participación Ciudadana de Tabasco o en el Padrón de Proveedores de Bienes Muebles y Servicios del Estado de Tabasco, interesadas en participar en la presente licitación.
Proveedor:	Persona física o jurídica colectiva que resulta adjudicada en la presente licitación y celebra un contrato de adquisiciones, arrendamientos o servicios con la Convocante.
Reglamento de la Ley:	Reglamento de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco.

2. GENERALIDADES DE LA LICITACIÓN

2.1. Origen de los recursos

Los compromisos que se generen serán cubiertos con cargo a los recursos federales, Ramo 28.- Participaciones a Entidades Federativas y Municipios, para el ejercicio fiscal 2024, autorizado al Instituto Electoral y de Participación Ciudadana de Tabasco para gasto electoral mediante el oficio SF/0065/2024, emitido por la Secretaría de Finanzas del Estado; correspondiéndole a la **Partida Presupuestal 31904.- Servicios integrales de infraestructura de cómputo**, del Programa Presupuestario **R002**.- Organización del Proceso Electoral del Estado de Tabasco, Proyecto.-

P004 Organización del proceso electoral, afectando el Componente **CRC03**.- Capitulo 3000 Servicios Generales.

2.2. Objeto de la licitación

La presente licitación tiene por objeto la contratación de los **Servicios Integrales de Infraestructura de Cómputo, Servicios de Seguridad, Nube e integración de Internet de los Edificios de las Juntas Electorales Distritales y Edificios Externos a la Red del IEPCT y Servicio de Sistema de CCTV y Monitoreo integrado,** a través del Licitante cuyas propuestas cumplan con las características y especificaciones técnicas señaladas en el **Anexo 5 "Especificaciones técnicas de los servicios a cotizar"** de las presentes Bases.

2.3. Información de la licitación

Toda la documentación emitida por los Licitantes en este procedimiento a la Convocante deberá ser dirigida al **Lic. Javier García Rodríguez, Presidente del Comité.**

El **Comité** tendrá a su cargo el procedimiento general de la licitación, por lo tanto, será el único facultado para desechar cualquier propuesta que no sea presentada conforme a lo dispuesto en la convocatoria, las presentes bases y sus anexos; resolverá los casos no previstos en la presente licitación e interpretará el contenido de las presentes bases.

La evaluación técnica estará a cargo del **Titular de la Unidad de Tecnologías de la Información y Comunicación de** la Convocante o del personal que éste designe.

Las oficinas del Convocante de la licitación se encuentran ubicadas en la Calle Eusebio Castillo N° 747, Col. Centro, en la Ciudad de Villahermosa, Tabasco, C.P. 86000:

Área Administrativa:	Coordinación de Recursos Materiales Tel: 99 33 58 10 00 extensión. 1070 y 1071 **Atención: M.A. Ángel Chan Solís**

Área Técnica:	Unidad de Tecnologías de la Información y Comunicación. Tel: 99 33 58 10 00 extensión. 1055 **Atención: Mtro. Raúl Olán León**

La Convocante proporcionará a todos los interesados, igual acceso a la información relacionada con los requisitos y condiciones que contengan las bases de la Licitación.

Ninguna de las condiciones contenidas en las presentes bases, así como las propuestas que presenten los Licitantes podrán ser negociadas.

Los Licitantes deberán asistir puntualmente a cada una de las etapas o actos de la presente licitación; **sólo se permitirá el acceso y participación de un representante por Licitante** que se encuentre inscrito.

Los Licitantes **no deberán utilizar teléfonos móviles** durante la celebración de cualquier etapa de la licitación; así mismo deberán guardar orden, respeto y buen comportamiento, en caso contrario, la Convocante podrá suspender el acto hasta que se restaure el orden, pudiendo solicitar al Licitante o Licitantes que abandonen el recinto. Si bien esto no es causal para efectos de descalificación, su cumplimiento es importante para la mejor conducción del procedimiento de que se trata.

El **Licitante** deberá apegarse estrictamente al contenido de estas bases de licitación, por lo que se recomienda leer detenidamente el contenido de estas, para evitar cualquier omisión que diera lugar a su descalificación en el transcurso de las distintas etapas del procedimiento.

La **Contraloría** verificará y aplicará el cumplimiento de la normatividad respectiva.

2.4. Aspectos económicos

Todos los costos que erogue el Licitante para su participación, preparación y presentación de sus propuestas, serán totalmente a su cargo, liberando a la Convocante de la obligación de reintegrarlos, cualquiera que sea el resultado de la presente licitación.

2.5. Costo, pago y disposición de las bases

Las presentes bases estarán a disposición de los interesados a partir del día de su **Publicación** el día 23 de marzo y la **venta de bases** del 23 al 27 de marzo de 2024; siendo responsabilidad exclusiva de los interesados adquirirlas oportunamente, las cuales tendrán un **costo de: $2,000.00 (dos mil pesos 00/100 m.n.)**, cuyo pago podrán realizarlo de la siguiente manera:

1. Mediante **DEPÓSITO** en Institución Bancaria *(La ficha de depósito deberá contener el sello del banco y rúbrica del cajero)* de conformidad con los siguientes datos:

1. Nombre del Titular de la Cuenta Bancaria: **INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO**.
2. Contrato: **8201815926**
3. Número de Cuenta: 7011-1946343.
4. CLABE Interbancaria: **002790701119463433.**
5. Institución Bancaria: **CITIBANAMEX.**

2. Mediante **transferencia electrónica,** de conformidad con los siguientes datos:

1. Nombre del Titular de la Cuenta Bancaria: **INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO**.
2. Concepto de pago: **Bases Licitación**
3. Referencia Numérica: **5627301**
4. Número de Cuenta: 7011-1946343.
5. CLABE Interbancaria: **002790701119463433.**
6. Institución Bancaria: **CITIBANAMEX.**

3. Mediante **pago en efectivo** en el área de Tesorería de la Coordinación de Recursos Financieros:

Área Tesorería: Coordinación de Recursos Financieros
Tel: 99 33 58 10 00 extensión. 1081 y 1014
Atención: C.P. Tilo Gómez Barahona.

Cabe señalar que, independientemente de que el pago se realice en la Institución Bancaria, ya sea con pago en ventanilla o mediante transferencia electrónica, el Licitante deberá presentarse en la Coordinación de Recursos Financieros del IEPCT con la ficha de depósito o el comprobante de la transferencia electrónica impresa, para que se le elabore un recibo simple, foliado con los datos de la Convocante. Y así acreditar su participación en la presente Licitación. Lo anterior deberá realizarlo en un horario de 10:00 a 15:00 horas, de lunes a domingo. Para este Instituto Electoral, en materia electoral todos los días y horas son hábiles, de acuerdo al artículo 154 numeral 1 de la Ley Electoral y de Partidos Políticos del Estado de Tabasco.

Las bases de la presente Licitación estarán disponibles en el Portal de CompraNet Tabasco de la Secretaría de la Función Pública del Gobierno del Estado, ingresando a la siguiente dirección: **portalanticorrupcion.tabasco.gob.mx:85/compranet/**, así como en la página institucional de la Convocante **iepct.mx**.

Para solicitar cualquier información al respecto, podrán comunicarse a los teléfonos 99 33 58 10 00 extensión. 1070 y 1071, en un horario de lunes a viernes de 10:00 a 15:00 horas.

El comprobante de pago por la adquisición de las bases será requisito indispensable para participar en la presente Licitación, en ningún caso, el derecho de participación será transferible.

No se aceptarán comprobantes ni fichas de depósito con fecha y hora posterior a la establecida como límite en el periodo de venta de bases, señalada en la convocatoria y en las presentes bases.

2.6. Forma y términos de facturación

El Licitante deberá entregar la factura debidamente requisitada y con los siguientes datos:

Nombre: Instituto Electoral y de Participación Ciudadana de Tabasco
Domicilio: Eusebio Castillo N° 747, Col. Centro, C.P.86000, Villahermosa, Tabasco.
RFC. IEP-961229-MTA.
Actividad Económica: Administración Pública Estatal en General.
Régimen: Personas Morales con Fines No Lucrativos.
Enviarla al: correo electrónico **facturacion@iepct.mx**

2.7. Precio y vigencia

Los precios deberán ser fijos y tener una vigencia durante el procedimiento de la Licitación, hasta la entrega total de los servicios, a entera satisfacción de la Convocante y por ningún motivo se podrá solicitar incrementos a los consignados en las propuestas presentadas y aceptadas, inclusive cuando exista ampliación en la vigencia del contrato y/o en las cantidades de los servicios originalmente solicitados hasta por el diez por ciento (10%) del monto total.

2.8. Traslado

El (los) Licitante (s) a quien (es) se le (s) adjudique el contrato derivado de la presente Licitación tendrá (n) bajo su cargo y responsabilidad el medio de transporte que consideren conveniente para el traslado de accesorios y equipamiento del servicio en las 21 Juntas Electorales Distritales (CATD), Oficinas Centrales del IEPCT, Edificio de la calle Hidalgo, Centro de Captura y Verificación (CCV), Almacén General y Edificio Sede (ubicaciones descritas en el **"ANEXO 5"**), por lo que esto no representará un costo adicional para la Convocante.

2.9. Etapas de evaluación

La evaluación de las propuestas que sean presentadas se realizará en (dos) 2 etapas:

En la **primera etapa**, se analizará y evaluará la Documentación Legal y Administrativa como primera instancia, la cual deberá ser presentada por fuera de los sobres. Posteriormente de darse fiel cumplimiento a los requisitos legales y administrativos, se procederá a la apertura de los sobres de las propuestas técnicas.

Se considerará que la propuesta del Licitante cumple con las especificaciones técnicas, si los servicios ofertados cubren con los requerimientos solicitados por la Convocante, mismos que se encuentran establecidos en el **"ANEXO 5"**, el cual forma parte de las presentes bases.

La Convocante se reserva el derecho de realizar visitas físicas a las instalaciones del (los) Licitante (s) que cumplan con lo solicitado en la etapa técnica, a fin de constatar la solvencia técnica y económica de los mismos.

En la **segunda etapa**, se evaluarán las propuestas económicas, considerando únicamente para este efecto la de los Licitantes cuyas propuestas no hubieran sido desechadas en la etapa técnica.

En ninguna de las etapas de evaluación de las propuestas se usarán mecanismos de puntos o porcentajes.

3. DOCUMENTOS REQUERIDOS PARA PARTICIPAR

3.1. Forma y términos para la presentación de propuestas

En el Acto de Presentación de Propuestas Técnicas y Económicas, y Apertura de Propuestas Técnicas, los Licitantes presentarán la **DOCUMENTACIÓN LEGAL ADMINISTRATIVA *a la vista, (fuera del sobre)***; la cual será revisada de forma cuantitativa para determinar si cumple o no con lo solicitado, lo anterior, con fundamento en el artículo 36 fracción V, párrafo segundo del Reglamento de la Ley.

La propuesta técnica y la propuesta económica de cada Licitante, se presentarán en ***sobres separados*** debidamente cerrados y sellados, ambos firmados de manera autógrafa por el representante legal, debidamente identificados como **PROPUESTA TÉCNICA Y PROPUESTA ECONÓMICA**, señalando los siguientes datos: Tipo de propuesta, número de licitación, razón social, domicilio, teléfono, nombre del representante legal y correo electrónico, con fundamento en los artículos 33 inciso a), fracción I de la Ley y 36 fracción V, párrafo primero del Reglamento de la Ley.

No se aceptará documentación legal administrativa en sobre o en caja cerrada o de otra naturaleza, la cual no permita verificar, visualizar o cotejar físicamente cada uno de los documentos que se solicitan.

3.2. Documentación legal administrativa (fuera de los sobres)

Los Licitantes deberán presentar en **ORIGINAL Y UNA COPIA SIMPLE LEGIBLE** de la documentación legal administrativa distinta a las propuestas. Las cuales se presentarán por separado; el juego original y el juego de copias.

La documentación se presentará en el orden que se enlista a continuación:

1. **Comprobante de pago de bases:** Será el recibo simple foliado que expida la Coordinación de Recursos Financieros de la Convocante.

   - **Para personas jurídicas colectivas:**

   1. Acta constitutiva y última reforma (en su caso), protocolizadas ante notario público e inscrita en el Registro Público de la Propiedad y el Comercio u oficina registral correspondiente, resaltando en la misma con marcador fluorescente, el o los párrafos donde señale su objeto social relacionado con el servicio a licitar.

2. Poder notarial del representante legal, resaltando en la misma con marcador fluorescente, el o los párrafos donde señale el nombre del representante legal, así como las facultades otorgadas a éste.

3. Identificación oficial con fotografía del representante legal, (credencial de elector, pasaporte, licencia de manejo, cartilla del servicio militar o cédula profesional).

4. Las personas que **NO** ostenten la representación legal de los Licitantes mediante poder notarial y que acudan al acto de presentación de propuestas técnicas y económicas, y apertura de propuestas técnicas, deberá presentar:

   a) Carta poder simple dirigida a la Convocante, en papel membretado, con firma y sello del Licitante, señalando claramente el nombre de la persona a quien se le autoriza participar en dicho acto, nombre y firma de quien acepta la representación y la de dos (2) testigos.

   b) Poder notarial que faculta a la persona que otorga el poder, resaltando en la misma con marcador fluorescente, el o los párrafos donde señale el nombre del representante legal, así como las facultades otorgadas a éste.

   c) Identificación oficial vigente de la persona que otorga y de quien recibe el poder, y en copia simple de los dos (2) testigos. (credencial de elector, pasaporte, licencia de manejo, cartilla del servicio militar o cédula profesional)

- **Para personas físicas:**

1. Acta de nacimiento (*actualizada*).

2. Identificación oficial con fotografía (credencial de elector, pasaporte, licencia de manejo, cartilla del servicio militar o cédula profesional).

3. El representante de la persona física que acuda al acto de presentación de propuestas técnicas y económicas, y apertura de propuestas técnicas, deberá presentar:

   a) Carta poder simple dirigida a la Convocante, en papel membretado, con firma y sello del Licitante, señalando claramente el nombre de la persona a quien se le autoriza participar en dicho Acto, nombre y firma de quien acepta la representación y la de dos (2) testigos.

   b) Identificación oficial vigente de la persona que otorga y de quien recibe el poder, así como de los 2 (dos) testigos. (credencial de elector, pasaporte, licencia de manejo, cartilla del servicio militar o cédula profesional)

- **Para ambos casos:**

1. Constancia de Situación Fiscal, con domicilio fiscal actualizado en el estado de Tabasco, **no mayor a dos (2) meses**. (*impresión del archivo electrónico descargado de la página del SAT con la actividad económica relacionada con el servicio, objeto de esta licitación*)

2. Comprobante de domicilio fiscal, **no mayor a dos (2) meses** (servicio de suministro de agua potable, energía eléctrica o servicio telefónico), el cual debe ser igual al domicilio registrado en la Constancia de Situación Fiscal; en caso de que el comprobante de domicilio no se encuentre a nombre del Licitante, deberá presentar también copia del contrato de arrendamiento correspondiente o manifestar mediante escrito, el hecho del porque no se encuentra el documento en cuestión a su nombre, el cual deberá acreditar con el documento donde está en trámite el cambio de domicilio ante la instancia correspondiente).

3. Cédula de Registro en el Directorio de Proveedores del Instituto Electoral y de Participación Ciudadana de Tabasco vigente, contemplando el Rubro **"038.- Servicio de Telecomunicaciones"**, o el **"13.- Equipos y Materiales de**

Comunicaciones" del Padrón de Proveedores de Bienes Muebles y Servicios del Estado de Tabasco vigente, para los servicios que se requieren en el **"ANEXO 5"** de las presentes bases.

4. Opinión del Cumplimiento de Obligaciones Fiscales **vigente**, **en sentido positivo**, emitida por el Servicio de Administración Tributaria **"SAT 32-D". (documento sujeto a verificación).**

5. Constancia de Cumplimiento de Obligaciones Fiscales Estatales **vigente**, **en sentido positivo**, emitida por la Secretaría de Finanzas del Estado de Tabasco **"34 Bis". (documento sujeto a verificación).**

(LA SIGUIENTE DOCUMENTACIÓN SE PRESENTARÁ EN ORIGINAL EN HOJA MEMBRETADA, CON SELLO DEL LICITANTE Y FIRMA DEL REPRESENTANTE LEGAL, EL CUAL, DEBERÁ ESTAR INTENGRADA EN EL JUEGO DE COPIAS):

6. Formato de Acreditamiento de la Personalidad. **"ANEXO 1".**

7. Escrito donde manifieste que acepta los términos de las bases y sus anexos. **"ANEXO 2".**

8. Escrito donde manifieste que no se encuentra en ninguno de los supuestos del Artículo 51 de la Ley. **"ANEXO 3".**

9. Escrito donde manifieste su declaración de integridad, prevista en el artículo 35, fracción II del Reglamento de la Ley **"ANEXO 4".**

10. Escrito relacionado con el cumplimiento de los servicios en cantidades, características y especificaciones, así como el cumplimiento a lo previsto en el artículo 53 de la Ley **"ANEXO 6".**

11. Escrito donde manifieste que cuenta con experiencia en el ramo.

12. Escrito en el que indique domicilio, teléfono y correo electrónico donde se les podrá hacer cualquier tipo de notificación.

Las copias simples que se solicitan en el presente numeral quedarán en poder de la Convocante, previo cotejo con el original respectivo, mismos que serán devueltos al (los) Licitante (s) una vez que concluya el Acto de Presentación de Propuestas Técnicas y Económicas, y Apertura de Propuestas Técnicas, con excepción de los originales señalados en los numerales del **6 al 12.**

3.3. Documentación técnica

Dentro del sobre de la Documentación Técnica deberá incluirse en **ORIGINAL EN HOJA MEMBRETADA**, con sello del Licitante y firma del representante legal en todas las hojas (igualmente cuando se presenten copias en ambos lados de la hoja), la siguiente documentación:

1. Propuesta Técnica, de conformidad con lo solicitado en el **"ANEXO 5"**, en el cual indique en los lotes que está ofertando, las características y especificaciones de los servicios.

   En el lote donde no presente propuesta, deberá incluir la leyenda **"NO COTIZO"**.

2. Escrito bajo protesta de decir verdad, donde manifieste que tiene plena capacidad de proporcionar la capacitación a operadores; la existencia de refacciones, instalaciones, equipo adecuado y personal competente para brindar el servicio y para respuesta inmediata en caso de alguna falla en el servicio, de conformidad con lo estipulado en el artículo 27, fracción XXI de la Ley.

3. Catálogos, folletos y/o fichas técnicas vigentes del fabricante que contengan de manera clara las características y especificaciones de los equipos que utilizarán en el servicio que ofertarán, en originales o copias simples legibles. El Licitante deberá identificar en los catálogos, folletos y/o fichas técnicas, el número del lote que le corresponde.

Lo anterior, con la finalidad de que el área requirente de la Convocante pueda verificar que las características que oferta el Licitante cumplen con lo solicitado en el **"ANEXO 5"**.

4. Escrito bajo protesta de decir verdad, donde manifieste que los equipos a utilizar en los servicios a ofertar, cumplen cabalmente con las características y requisitos establecidos en las normas oficiales mexicanas aplicables para los equipos de tecnologías de la información.

Los documentos deberán ser presentados en el idioma español, de conformidad con el Artículo 27 fracción V de la Ley, en caso de estar en otro idioma deberá encontrarse la respectiva traducción al español.

3.4. Documentación económica

Dentro del sobre de la Documentación Económica deberá incluirse en **ORIGINAL EN HOJA MEMBRETADA**, con sello del Licitante y firma del representante legal en todas las hojas (igualmente cuando se presenten copias en ambos lados de la hoja), la siguiente documentación:

1. Propuesta Económica, de conformidad con el **"ANEXO 7"**, la cual se presentará sin correcciones, raspaduras o enmendaduras, estableciendo con claridad **el precio unitario, incluyendo el descuento (en caso de existir), importe, subtotal, Impuesto al Valor Agregado y total.**

   Los precios deberán estar expresados en moneda nacional y ajustándolos a las unidades de pesos y centavos; el precio unitario no deberá incluir el IVA, éste impuesto se agregará a la suma final de la Oferta Económica. La propuesta económica deberá presentarse **a dos decimales, en caso contrario será desechada.** Preferentemente deberá proteger con cinta adhesiva transparente toda la columna de importe incluyendo el subtotal, IVA y total.

2. Escrito mediante el cual establezca las condiciones de la oferta, de conformidad con lo solicitado por la Convocante:

a) Lugar de entrega:

Para los servicios Integrales de Infraestructura de Cómputo, Servicios de Seguridad, Nube e Integración de Internet de los Edificios de las Juntas Electorales Distritales y Edificios Externos a la Red del IEPCT (ubicaciones descritas en el **"Anexo 5"**).

1. Oficinas Centrales del Instituto Electoral y de Participación Ciudadana de Tabasco.
2. (21) Juntas Electorales Distritales CATD (Centro de acopio y transmisión de datos).
3. Edificio Méndez CCV (Centro de captura y verificación).
4. Edificio de Hidalgo.
5. Almacén General del IEPCT.
6. Edificio Sede Periférico (CATD para caso fortuito o fuerza mayor).

Para los Sistemas de CCTV (Control De Circuito Cerrado De Televisión) y Servicio de Monitoreo Integrado, los sitios de entrega serán los siguientes (ubicaciones descritas en el **"Anexo 5"**):

1. Oficinas Centrales (Servicio de Monitoreo Integrado).
2. (21) Juntas Electorales Distritales CATD (Centro de acopio y transmisión de datos).
3. Edificio Méndez CCV (Centro de captura y verificación).
4. Edificio Sede Periférico (CATD para caso fortuito o fuerza mayor).

b) Tiempo de entrega: Deberá manifestar bajo protesta de decir verdad que se compromete a empezar la entrega de los servicios en un término de 15 días naturales, contados a partir del día siguiente hábil de la suscripción del contrato correspondiente. Por lo tanto, el tiempo que proponga el (los) Licitante (s), no deberá exceder del establecido por la Convocante.

c) **Forma de entrega:** Servicio debidamente instalado, configurado, activado y operando, con equipos nuevos y en perfecto estado, sin fallas y sin vicios ocultos.

d) **Condiciones de pago:** El pago se realizará de forma mensual, en moneda nacional, mediante transferencia electrónica, dentro de los 20 días naturales posteriores a la presentación de la factura que deberá reunir los requisitos fiscales correspondientes, a entera satisfacción de la Convocante.

3. **Cheque de garantía** de seriedad de la propuesta, de conformidad con lo señalado en el numeral **5.1.** de las presentes bases.

4. Incluir en medio magnético su propuesta económica (USB). El archivo de la Oferta Económica deberá estar elaborada en Formato Excel, sin contraseñas o candados.

5. Escrito mediante el cual se compromete que los **precios serán fijos** y tendrán una **vigencia** durante el proceso de la Licitación hasta la recepción final de los servicios, a entera satisfacción de la Convocante y por ningún motivo se podrán solicitar incrementos a los consignados en las propuestas presentadas; inclusive cuando exista ampliación en la vigencia del contrato y/o en las cantidades de los servicios originalmente solicitados hasta por el diez por ciento (10%) del monto total.

Los documentos deberán ser presentados en el idioma español, de conformidad con el Artículo 27 fracción V de la Ley.

4. PROCEDIMIENTO Y ACTOS DE LA LICITACIÓN

Los Licitantes participantes **en cada uno de los actos** de esta Licitación, deberán presentarse 30 minutos antes de cada acto, en las fechas y horarios establecidos en el calendario de actos **"ANEXO 9"**, para efectos de registrarse de manera oportuna. Una vez iniciados los Actos, no se aceptará la participación de los Licitantes que lleguen después de la hora fijada.

Todos los actos de la presente Licitación se realizarán en la **Sala de Sesiones "Mtro. Roberto Félix López"** ubicada en las instalaciones de la Convocante, en Calle Eusebio Castillo N° 747, Col. Centro, en Villahermosa Tabasco, en las fechas y horarios establecidos en el calendario de actos **"ANEXO 9"**.

4.1. Junta de aclaraciones

1. Cualquier Licitante podrá solicitar aclaraciones sobre las bases de la Licitación y las especificaciones técnicas relacionadas con la misma. Las preguntas deberán ser enviadas mediante correo electrónico a las direcciones **angel.chan@iepct.mx** y **coordrecursosmateriales@iepct.mx**, conforme a lo señalado en el **"ANEXO 10"**, en el horario y fechas señaladas en el calendario de actos **"ANEXO 9"**.

   Las preguntas deberán enviarse en Formato Word, sin contraseñas o candados, no se aceptarán las preguntas de los Licitantes que lo envíen en un formato distinto al solicitado; de igual manera, se tendrán como no enviados los archivos que contengan virus y por seguridad el servidor de la Convocante los indique como de dudosa procedencia y los envíe al spam, por lo que el Licitante deberá de confirmar la debida recepción de sus preguntas al teléfono **99 33 58 10 00 ext. 1070 y 1071**.

2. Los Licitantes deberán adjuntar a las preguntas que realicen, copia del comprobante de pago de bases. La Convocante acusará de recibido la recepción de las preguntas enviadas en tiempo y forma. Sólo se le dará respuesta a las preguntas de los Licitantes que hayan enviado copia del pago de bases de la presente Licitación.

3. Las respuestas a las preguntas técnicas enviadas por los Licitantes, notas aclaratorias y modificaciones, conforme a las especificaciones técnicas señaladas en el **"ANEXO 5"**, correrán a cargo de la **Unidad de Tecnologías de la Información y Comunicación**, en tanto que las preguntas de carácter legal y administrativo correrán a cargo de la Convocante, según aplique.

4. La asistencia a este acto será opcional para los Licitantes, pero los acuerdos que se tomen en ésta serán obligatorios para todos.

5. En el desarrollo de este acto, de conformidad con lo señalado en el primer punto del presente numeral, la Convocante sólo dará lectura a las respuestas de las preguntas formuladas en tiempo y forma por los Licitantes, quienes podrán solicitar aclaraciones única y exclusivamente sobre las mismas durante la reunión, por lo tanto, no podrán formular preguntas nuevas.

6. Los Licitantes que asistan a este acto, deberán presentar copia simple del comprobante de pago de las bases de la presente Licitación, el cual deberá ser entregado al momento en que se registren en la lista de asistencia.

7. Las aclaraciones a las bases y a las especificaciones técnicas que se deriven de la junta de aclaraciones se asentarán en el acta que se elabore al efecto, la que contendrá la firma de los asistentes. La omisión de firma del acta por parte de alguno de los Licitantes asistentes no invalidará el contenido de la misma. Se entregará copia del acta a cada uno de los Licitantes que haya asistido a la reunión. Los que no hayan asistido a esta Junta, podrán descargar el acta desde el Sistema CompraNet Tabasco, la página institucional de la Convocante o en su caso, solicitar copia simple mediante escrito dirigido al Presidente del Comité.

4.2. Acto de presentación de propuestas técnicas y económicas, y apertura de propuestas técnicas

1. El acto de presentación de propuestas técnicas y económicas, y apertura de propuestas técnicas, se llevará a cabo en la fecha señalada en el calendario de actos, **"ANEXO 9"** de las presentes bases.

2. Los Licitantes deberán presentar a la vista, la documentación legal administrativa solicitada en el numeral **3.2.**, así como sus respectivas propuestas en dos sobres cerrados

en forma inviolable, uno con la propuesta técnica y otro con la propuesta económica, de conformidad con lo solicitado en los numerales **3.3. y 3.4**.

3. Se recibirá y revisará la documentación legal administrativa de forma cuantitativa requerida en términos de lo señalado en el punto anterior, para su posterior evaluación cualitativa; **se descalificará** la documentación de los Licitantes que hubieren omitido alguno de los requisitos solicitados, por lo cual, no se aperturarán sus propuestas técnicas ni económicas. (No será motivo de descalificación la omisión por parte del Licitante de resaltar con marcador fluorescente el objeto social, nombre del representante legal y facultades otorgadas)

4. En caso de que el Licitante cumpla de manera satisfactoria con la documentación legal administrativa, se procederá a abrir el sobre que contiene la propuesta técnica exclusivamente, para verificar que la información solicitada se presente completa, de conformidad con el **punto 3.3.** de las presentes bases.

5. La documentación de la propuesta técnica se recibirá de forma cuantitativa, para su posterior evaluación cualitativa y análisis técnico. El titular del área técnica o el personal que designe elaborará un dictamen o fallo técnico donde hará constar el cumplimiento o incumplimiento de las propuestas presentadas para cada uno de los lotes en cuanto a los aspectos técnicos, el cual será suscrito por el responsable de la revisión. El resultado del análisis de las propuestas técnicas se hará del conocimiento de los Licitantes mediante la lectura del dictamen o fallo técnico en el acto de lectura del fallo técnico y apertura de propuestas económicas, en la fecha señalada en el Calendario de Actos **"ANEXO 9"**.

6. Los Licitantes que deseen hacerlo o por lo menos dos (2) representantes nombrados por éstos dentro de los presentes y los integrantes del Comité rubricarán al final de la reunión todas las propuestas técnicas presentadas, así como los sobres cerrados de las propuestas económicas, para garantizar su inviolabilidad; quedando los sobres cerrados como originalmente se presenten en custodia de la Convocante, para que sean abiertos

en el acto de lectura del fallo técnico y apertura de propuestas económicas, de conformidad con lo estipulado en el artículo 33, inciso a), fracción II de la Ley.

7. Se levantará acta en dos (2) tantos originales, en la que se hará constar las propuestas técnicas presentadas y las observaciones que sean pertinentes, firmándose por todos los Licitantes presentes y los integrantes del Comité. La omisión de firmas por parte de alguno de los Licitantes no invalidará su contenido y efecto, entregándose a cada uno de éstos copia simple del acta.

8. Al finalizar el presente acto, a los Licitantes se les hará la devolución de los documentos originales presentados en la documentación legal administrativa.

4.3. Acto de lectura de fallo técnico y apertura de propuestas económicas

1. El acto de lectura de fallo técnico y apertura de propuestas económicas se llevará a cabo en la fecha y hora señaladas en el calendario de actos **"ANEXO 9"** de las bases.

2. Se dará lectura al dictamen o fallo técnico emitido por el área requirente, señalando el cumplimiento o las causas de incumplimiento de las propuestas aceptadas por cada uno de los lotes o partidas, de conformidad con las especificaciones técnicas solicitadas en el **"ANEXO 5"** y posteriormente se realizará la apertura de las propuestas económicas de los Licitantes cuyas propuestas técnicas no hayan sido desechadas.

3. Únicamente se dará lectura en voz alta de los importes totales de aquellas propuestas económicas que cumplan con los requisitos solicitados en el **punto 3.4.** de las presentes bases, de conformidad con lo señalado en los artículos 33 inciso b), fracción II de la Ley y el 36, fracción V, inciso B), segundo párrafo del Reglamento de la Ley.

4. Posteriormente, con base en el dictamen o fallo técnico emitido por el área requirente, las propuestas económicas admitidas y considerando el presupuesto autorizado, se elaborará el cuadro comparativo y se procederá al análisis económico correspondiente

para su adjudicación. El cuadro comparativo deberá ser firmado por los integrantes del Comité.

5. Los Licitantes que deseen hacerlo o por lo menos dos (2) representantes nombrados por éstos dentro de los presentes y los integrantes del Comité rubricarán al finalizar la reunión todas las propuestas económicas aceptadas.

6. Se levantará acta en dos (2) tantos originales, en la que se dará constancia de las propuestas económicas aceptadas y los motivos de las que hubieren sido desechadas en este acto, firmándose por todos los Licitantes asistentes y los integrantes del Comité; la omisión de firmas por parte de los Licitantes no invalidará su contenido y efectos, entregándose copia simple del acta a cada uno de ellos.

4.4. Criterios que se aplicarán en la evaluación y adjudicación

Cuando exista diferencia entre la cantidad de servicios ofertados por el Licitante y las solicitadas por la Convocante en el **"ANEXO 5"**, se tomará como válida la contemplada en este último. Asimismo, cuando existan errores en las operaciones aritméticas de las propuestas económicas de los Licitantes, se corregirán los importes en el cuadro comparativo correspondiente y la suma total que resulte será la que se tome como correcta para efectos del análisis correspondiente, sin modificar los precios unitarios presentados.

La adjudicación de la presente Licitación se realizará por lote, en todo caso, se adjudicará a la propuesta solvente más baja, siempre que cumpla con las condiciones legales, técnicas y económicas requeridas por la Convocante, de conformidad con lo estipulado en el artículo 34 de la Ley.

En caso de empate en el precio entre dos o más propuestas, la adjudicación se efectuará mediante sorteo que celebre la Convocante en el propio acto de fallo, el cual consistirá en la colocación de un boleto por cada propuesta que resulte empatada y serán depositadas en

una urna, de la que se extraerá el boleto del Licitante ganador, de conformidad con lo previsto en el artículo 36, fracción V, inciso B), último párrafo del Reglamento de la Ley.

4.5. Fallo de la licitación

Este acto se llevará a cabo en la fecha y hora señaladas en el calendario de actos **"ANEXO 9"** de las presentes bases. Se levantará el acta del fallo de la Licitación en dos (2) tantos originales, la cual contendrá los datos del Licitante (es) Adjudicado (s), lote (s) e importe (s) y total (es) asignados con el impuesto al valor agregado incluido. Dicha acta será firmada por todos los Licitantes presentes y los integrantes del Comité, entregándose copia simple del acta a cada uno de los Licitantes. La omisión de firma por parte de los Licitantes no invalidará su contenido y efectos.

Contra la resolución que contenga el Fallo, no procederá recurso alguno de impugnación durante el acto administrativo del proceso licitatorio de que se trate.

En sustitución de esta Junta, la Convocante podrá optar por notificar el Fallo de la Licitación por escrito a cada uno de los Licitantes o enviarlo al correo electrónico que hayan proporcionado para efectos de notificación, debiendo acusar de recibido el mismo, dentro de un término que no podrá exceder de quince (15) días hábiles, contados a partir de la fecha de celebración del acto de lectura del fallo técnico y apertura de propuestas económicas.

4.6. Causas de cancelación, declaración desierta, diferimiento de actos y reducción en la cantidad de servicios a adquirir

El Comité podrá cancelar, declarar desierta la Licitación en su totalidad o en determinados lotes, reducir la cantidad de servicios a adquirir, así como diferir por una sola vez cualquier acto del procedimiento, en los siguientes casos:

1. **Cancelación.** El Comité se reserva el derecho de cancelar definitivamente en cualquier momento la presente Licitación, hecho que se notificará a todos los Licitantes por escrito, en los siguientes casos:

   I. Cuando se extinga la necesidad de adquirir los servicios señalados en el **"ANEXO 5"**;

   II. Cuando de continuar con el procedimiento se pudiera ocasionar un daño o perjuicio a la Convocante; y

   III. Por no convenir a los Intereses de la Convocante.

2. **Desierta.** El Comité podrá declarar desierta la Licitación en su totalidad o en determinados lotes, cuando:

   I. No se reciban proposiciones en el Acto de Presentación de Propuestas Técnicas y Económicas, y Apertura de Propuestas Técnicas;

   II. Las proposiciones presentadas no reúnan las condiciones legales, técnicas y económicas solicitadas en las bases; y

   III. Si se considera que las proposiciones presentadas no convienen a los intereses de la Convocante.

3. **Diferimiento.** La Convocante podrá diferir por una sola vez cualquier acto de la Licitación cuando así convenga a sus intereses, fundando y motivando debidamente tal decisión.

4. **Reducción de lotes.** La Convocante se reserva el derecho de reducir las cantidades a adquirir en determinados lotes de la presente Licitación, cuando se advierta que existe insuficiencia presupuestal.

4.7. Causas de descalificación

El Comité descalificará las propuestas de los Licitantes, cuando:

1. No presenten las propuestas en la hora fijada en las presentes bases;

2. No presenten alguna documentación o no cumplan con alguno de los requerimientos solicitados en los numerales **3.2., 3.3. y 3.4.**, en la forma señalada;

3. No establezcan con claridad algún concepto o especificación en las propuestas técnica y económica;

4. No presenten firma autógrafa del representante legal y/o sello de la empresa en la documentación legal, así como en la propuesta técnica y económica;

5. El importe del cheque de garantía de seriedad de la propuesta económica sea inferior al 5% solicitado u omita algún dato de los señalados en el numeral **5.1.** de las presentes bases;

6. La propuesta económica no se presente en moneda nacional;

7. Las propuestas no sean redactadas en idioma español;

8. Se encuentren impedidos para participar en términos del Artículo 51 de la Ley;

9. Propongan más de una opción del bien ofertado;

10. Incluyan el Impuesto al Valor Agregado en el (los) precio (s) unitario (s) de la oferta económica;

11. No garantice plenamente la calidad de los servicios, de conformidad con lo solicitado por el área requirente;

12. Que no considere los acuerdos derivados de la Junta de Aclaraciones; y

13. Cualquier otra causa que contravenga las disposiciones legales que rigen la presente base, así como la comprobación de que algún Licitante ha acordado con otro elevar los precios de los servicios integrales de infraestructura y arrendamiento de sistema de CCTV

o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás Licitantes.

4.8. Devolución de propuestas y cheques de garantía

El procedimiento de devolución de propuestas técnicas y económicas descalificadas que no fueron aperturadas, así como los cheques en garantía de los Licitantes que no resulten adjudicados o en caso de que se declare desierta la Licitación, correrán a cargo de la Coordinación de Recursos Materiales adscrita a la Dirección de Administración, en un término de **quince (15)** días naturales posteriores a la fecha del fallo de la Licitación, con excepción de los Licitantes que presenten inconformidades, a quienes se les reintegrará **quince (15)** días naturales posteriores a la notificación de las partes del acuerdo en el que se declare que ha quedado ejecutoriada la resolución o ha causado estado la misma.

Para los Licitantes que resulten adjudicados en el fallo de la licitación, se les retendrá el cheque con el que se garantiza el sostenimiento de su propuesta económica, hasta el momento en que presenten la garantía de cumplimiento (Fianza) del contrato correspondiente.

Las propuestas técnicas y económicas que fueron aperturadas y cumplieron con lo solicitado, quedan en poder de la Convocante.

5. DOCUMENTOS DE GARANTÍA

5.1. Garantía de seriedad de la propuesta económica (cheque)

Para garantizar la seriedad de las Propuestas Económicas, los Licitantes deberán incluir en la misma, un cheque no negociable con la Leyenda "**Para abono en cuenta del Beneficiario**", por un importe mínimo del cinco por ciento **(5%) del total sin IVA de la oferta económica**, a favor del **Instituto Electoral y de Participación Ciudadana de Tabasco**, de conformidad con lo estipulado en el artículo 31, fracción I de la Ley; en caso de que no se pueda colocar el nombre completo, abreviarlo como Inst. Elect. y de Part. Ciud. de Tab.,

El cheque **no deberá ser perforado ni engargolado o adherido a algún papel** y deberá incluir entre otros datos los siguientes: cuenta del Licitante, fecha, número de cheque, nombre del beneficiario, importe con número, importe con letra, firma del cuentahabiente. **El cheque deberá ser debidamente requisitado, en caso contrario, será motivo de descalificación.**

5.2. Garantía de cumplimiento (fianza)

El (los) Licitante (s) que resulten beneficiados con la adjudicación del (los) lote (s) objeto de la presente Licitación, deberán garantizar el cumplimiento del contrato, otorgando una **fianza por el veinte por ciento (20%) del monto total adjudicado, incluido el IVA**., la cual deberá estar vigente por el período de un (1) año, a partir de su emisión, a favor de la Convocante.

En caso de incumplimiento a los términos del contrato fincado, la Convocante podrá aplicar esta garantía, aun cuando se haya suministrado parcialmente los servicios.

La fianza de cumplimiento deberá exhibirse dentro del plazo de diez (10) días naturales contados a partir de la fecha de firma del contrato, debiendo cumplir con las formas y términos previstos en los artículos 32, fracción III de la Ley y 19 del Reglamento de la Ley, conforme a lo señalado en el **"ANEXO 7".**

5.3. Ejecución de garantías

1. Se harán efectivas las garantías relativas al sostenimiento de la oferta económica (cheque), en los siguientes casos:

   a) Cuando los Licitantes no sostengan sus propuestas;

   b) Cuando el Licitante no firme el contrato correspondiente en un plazo máximo de veinte (20) días hábiles, contados a partir de la notificación del fallo; y

   c) No entregue la fianza de cumplimiento en el plazo estipulado en la Ley.

2. Se harán efectivas las garantías relativas al cumplimiento del contrato (fianza), en los siguientes casos:

   a) Cuando hubiese transcurrido el tiempo máximo convenido para la entrega de los servicios;

   b) Por no cumplir los servicios con las especificaciones técnicas y de calidad establecidas en su propuesta; y

   c) Cuando hubiese transcurrido el plazo que se concede al Licitante para efectuar los cambios necesarios, cuando los servicios no cumplan con lo solicitado.

Adicionalmente a las sanciones anteriormente señaladas, serán aplicables las previstas por los ordenamientos legales vigentes en la materia.

6. CONTRATO

6.1. Generalidades

El contrato se suscribirá en la Coordinación de Recursos Materiales, ubicada en la dirección de la Convocante, en días hábiles, de lunes a viernes, en horario de **10:00 a 15:00 horas**, en un término de hasta veinte (20) días hábiles, contados a partir de la fecha de la notificación del fallo, para lo cual el Licitante adjudicado deberá presentar la Póliza de Fianza.

Los derechos y obligaciones que se deriven de los contratos, en ningún caso, podrán cederse en todo o en parte a otras personas físicas o jurídicas colectivas, con excepción de los derechos de cobro sobre los pagos pendientes de cubrirse, en cuyo caso, se deberá contar con la aprobación previa y por escrito de la Convocante.

6.2. Penas convencionales

Una vez celebrado el contrato, si el Licitante adjudicado incumple con las condiciones establecidas en el mismo para la entrega de los servicios, se le aplicará una pena convencional equivalente al **0.3 por ciento** por cada día de atraso, sobre el importe de los servicios que se encuentren en situación de incumplimiento, hasta por el veinte por ciento (20%) de la garantía de cumplimiento. Dicha sanción se establecerá en el contrato respectivo.

6.3. Devoluciones al Proveedor

La Convocante mediante escrito realizará la devolución de los bienes que forman parte del servicio al proveedor en el supuesto de que se detecten vicios ocultos, defectos de fabricación, fallas o la falta de calidad en general durante su uso y dentro del período de garantía solicitado por el área requirente. Por lo tanto, en términos del artículo 55, fracción III, del Reglamento de Ley, el proveedor se obliga a reponerlos a entera satisfacción del área requirente, para lo cual tendrá un plazo no mayor de **quince (15)** días naturales, contados a partir del día siguiente hábil en que se le notifique alguna eventualidad, sin que ello genere costos adicionales para la Convocante.

6.4. Cantidades adicionales y ampliación de vigencia por modificaciones a los contratos

Dentro del presupuesto aprobado y disponible, la Convocante podrá modificar los contratos, de conformidad con lo establecido en los artículos 43 de la Ley y 58 del Reglamento de la Ley, en los siguientes casos:

1. Por ampliación de la vigencia; y

2. Por incremento en la cantidad de los servicios informáticos y de sistema de CCTV y monitoreo integrado originalmente adquiridos, hasta por monto equivalente al **diez por ciento (10%)** del monto total del contrato.

Los convenios modificatorios respectivos, serán suscritos por los servidores públicos y Licitantes que lo hayan hecho en el contrato original o por quienes los sustituyan. La Convocante se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos no previstos en bases, especificaciones, y en general, cualquier cambio que implique otorgar mejores condiciones para el Licitante, comparadas con las establecidas originalmente.

6.5. Rescisión y suspensión

Procederán las rescisiones de los contratos, cuando el (los) Licitante (s) incumplan con las obligaciones a su cargo, como en los siguientes casos:

1) Cuando el (los) Licitante (s), modifique (n) las características o especificaciones de los servicios de nube, infraestructura, seguridad y servicio del sistema de CCTV y monitoreo integrado adquiridos;
2) Por incumplimiento de cualquiera de las obligaciones a cargo del (los) Licitante (s);
3) Cuando concurran razones de interés general; y
4) Cuando por causas justificadas debidamente fundadas y motivadas, se extinga la necesidad de requerir los servicios contratados.

Podrá suspenderse administrativamente o darse por terminado anticipadamente el contrato, cuando para ello concurran razones de interés general, o bien, cuando por causas justificadas debidamente fundadas y motivadas, se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que, de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a la Convocante.

El procedimiento que se observará para ambos casos será conforme lo que marca el artículo 49 de la Ley y las demás disposiciones legales aplicables.

6.6. De la Inhabilitación del (los) Licitante (s)

Adicionalmente a las anteriores sanciones, el (los) Licitante (s) que cometan determinadas infracciones en relación con la adquisición de los servicios adquiridos en la Licitación, se harán acreedores a la inhabilitación para participar en los procedimientos de contratación o celebración de contratos, entre otras de las sanciones que establecen los artículos 66 y 67 de la Ley.

6.7. De las inconformidades y controversias

Contra la resolución que contenga el fallo, no procederá recurso alguno durante el acto administrativo del proceso licitatorio de que se trate.

Los Licitantes podrán inconformarse por escrito ante la Contraloría de la Convocante, en relación a cualquier etapa o fase de la Licitación, antes del fallo de la adjudicación y por actos posteriores al fallo que impliquen la imposición de condiciones diferentes a la de la convocatoria y de las bases, dentro de un plazo de diez días hábiles siguientes al que tenga conocimiento.

El procedimiento que deberá observarse para efectuar las inconformidades será conforme lo estipulado en el Artículo 71 de la Ley.

La manifestación de hechos falsos se sancionará conforme a las disposiciones legales aplicables.

Atentamente

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
IEPC TABASCO
COMITÉ DE COMPRAS

Lic. Javier García Rodríguez
Presidente del Comité de Compras del Instituto Electoral y de Participación Ciudadana de Tabasco

"ANEXO 1"

ACREDITAMIENTO DE LA PERSONALIDAD

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO
ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Bajo protesta de decir verdad, manifiesto que los datos aquí asentados son ciertos y cuento con las facultades suficientes para suscribir la propuesta en la presente Licitación Pública Estatal N°_____, a nombre y representación de: (NOMBRE DE LA EMPRESA).

REGISTRO FEDERAL DE CONTRIBUYENTES:
DOMICILIO (CALLE Y NÚMERO):
COLONIA: DELEGACIÓN O MUNICIPIO:
CÓDIGO POSTAL: ENTIDAD FEDERATIVA
TELÉFONOS: FAX:
CORREO ELECTRÓNICO
N° DE LA ESCRITURA PÚBLICA EN LA QUE CONSTA SU ACTA CONSTITUTIVA:
VOLUMEN FECHA:
NOMBRE, NÚMERO Y LUGAR DEL NOTARIO PÚBLICO ANTE EL CUAL SE DIO FE DE LA MISMA:
RELACIÓN DE ACCIONISTAS.-
APELLIDO PATERNO: APELLIDO MATERNO NOMBRE (S)
DESCRIPCIÓN DEL OBJETO SOCIAL:
REFORMAS AL ACTA CONSTITUTIVA:

NOMBRE DEL APODERADO O REPRESENTANTE LEGAL:
DATOS DEL DOCUMENTO MEDIANTE EL CUAL ACREDITA SU PERSONALIDAD Y FACULTADES.-
ESCRITURA PÚBLICA NÚMERO: LIBRO FECHA
NOMBRE, NÚMERO Y LUGAR DEL NOTARIO PÚBLICO ANTE EL CUAL SE OTORGO:
(LUGAR Y FECHA)

PROTESTO LO NECESARIO

_____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

Nota: El presente formato podrá ser reproducido por cada participante en la manera que estime conveniente, debiendo respetar su contenido, preferentemente, en el orden indicado.

"ANEXO 2"

ACEPTACIÓN DE TÉRMINOS DE LAS BASES

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Yo _____ en mi carácter de representante legal de la empresa denominada _____, manifiesto a Usted lo siguiente:

Que el suscrito y las personas que forman parte de la sociedad y de la propia empresa que represento, nos sujetaremos al procedimiento establecido en las bases de la Licitación Pública Estatal N° _____, relativa a los servicios de _____. Por lo tanto, acepto íntegramente las condiciones establecidas en las mismas y en sus Anexos, así como las modificaciones y acuerdos que pudieran derivarse en el Acto de la Junta de Aclaraciones de la presente Licitación. Asimismo, le expreso que conozco la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco, y el Reglamento de la Ley.

PROTESTO LO NECESARIO

_____

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

"ANEXO 3"

MANIFESTACIÓN DE NO ENCONTRARSE EN ALGUNO DE LOS SUPUESTOS DEL ARTÍCULO 51 DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y PRESTACIÓN DE SERVICIOS DEL ESTADO DE TABASCO

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Yo _____ en mi carácter de representante legal de la empresa denominada _____, declaro bajo protesta de decir verdad lo siguiente:

Que el suscrito y las personas que forman parte de la sociedad y de la propia empresa que represento, no nos encontramos en alguno de los supuestos señalados en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y prestación de Servicios del Estado de Tabasco y lo manifiesto para los efectos legales correspondientes, en relación con la presente Licitación Pública Estatal N° _____, relativa a la contratación Servicios Integrales De Infraestructura De Cómputo.

PROTESTO LO NECESARIO

_____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

"ANEXO 4"

DECLARACIÓN DE INTEGRIDAD

ARTÍCULO 35, FRACCIÓN II DEL REGLAMENTO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y PRESTACIÓN DE SERVICIOS DEL ESTADO DE TABASCO

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Yo _____, representante legal de la Empresa_____, me permito señalar que respecto a la Licitación Pública Estatal N° _____, relativa a los servicios informáticos y de sistema de CCTV y monitoreo integrado, manifiesto bajo protesta de decir verdad, lo siguiente:

Que el suscrito y las personas que forman parte de la sociedad y de la propia empresa que represento o a través de interpósita persona, nos abstendremos de adoptar conductas que induzcan a que los servidores públicos de la Convocante alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que otorguen condiciones más ventajosas con relación a los demás participantes, de conformidad con lo establecido por el artículo 35 fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco.

Por lo anteriormente expuesto, solicito que se tenga por presentada en tiempo y forma a mi representada en la presente Licitación Pública Estatal.

PROTESTO LO NECESARIO

_____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

"ANEXO 5"

Villahermosa, Tabasco a 20 de marzo de 2024.

31904.- Servicios Integrales de Infraestructura de Cómputo
REQUISICIÓN DA/CRM/151/2024
LOTE 1

Lote	Descripción	Cantidad Total	Sitios requeridos	Periodo de uso
1	Servicio de conectividad para la red **WAN**, **LAN**, integración e instalación de la **red de voz y datos** de los edificios externos con las oficinas centrales. Debe incluir: • **30** Firewalls UTM (Administración Unificada de Amenazas) • **4** Firewalls UTM (Administración Unificada de Amenazas) alta disponibilidad. • **52** Access Points. • **26** Switches de datos de 24 puertos 12 Puertos 1 Gigabit Ethernet RJ45 y 12 Puertos 1 Gigabit E RJ45 Power Over Ethernet (POE) • **1** Switch de 48 puertos 24 Puertos 1 Gigabit Ethernet RJ45 y 24 Puertos 1 Gigabit E RJ45 Power Over Ethernet (POE) • Servicios de instalación, configuración, capacitación y monitoreo. • Soporte técnico remoto y en sitio. • Ingenieros certificados con la arquitectura y la marca. • Servicio de cómputo en la nube para 9 instancias y servicio de bases de datos relacional, para los sistemas SIEE (Sistema de Información Estatal Electoral, Pruebas y Capacitación (SIEE), PREPET (Programa de Resultados Preliminares del Estado de Tabasco), PREP Casilla, Pagina WEB, CONÓCELES, DNS. ***(Se anexa ficha técnica de los requerimientos)***	1	21 Juntas Electorales Distritales (CATD) Oficinas Centrales Edificio de Hidalgo Centro de captura y verificación (CCV) Almacén General Edificio Sede Oficinas Centrales del IEPC Tabasco	25 abril al 30 de junio de 2024

FICHA TÉCNICA DEL LOTE 1

SERVICIOS INTEGRALES DE INFRAESTRUCTURA DE COMPUTO, SERVICIOS DE SEGURIDAD, NUBE E INTEGRACIÓN DE INTERNET DE LOS EDIFICIOS DE LAS JUNTAS ELECTORALES DISTRITALES Y EDIFICIOS EXTERNOS A LA RED DEL IECPT

La presente sección específica las características técnicas que el Instituto Electoral y de Participación Ciudadana de Tabasco requiere para dar cumplimiento a las necesidades de aprovisionamiento de los **Servicios Integrales de Infraestructura de Cómputo, Servicios de Seguridad, Nube e Integración de Internet de los Edificios de las Juntas Electorales Distritales y Edificios Externos a la Red del IEPCT** que se describen en la presente sección.

Los servicios antes mencionados deberán ser adjudicados a un solo Licitante, por lo que las propuestas técnicas y económicas presentadas deberán considerar, el total de instancias y base de datos para los servicios de nube, servicios de seguridad y el total de sitios para los servicios de integración de equipos para la interconexión de las oficinas centrales y los edificios externos, no se aceptarán propuestas que solo consideren parte de los servicios de la presente licitación, ya que es recomendable adjudicar a un solo proveedor por cuestiones técnicas, monitoreo, configuración, interacción con los sitios en las mesas de ayuda y soporte.

El proveedor de servicios deberá considerar en su propuesta técnica económica un periodo de contratación de los servicios mencionados por el periodo solicitado, con soporte garantías del servicio durante la vigencia del contrato en cada una de las ubicaciones del Instituto indicadas en el ***ANEXO 1.1 Listado de Sitios para su integración de equipos*** del presente documento.

ANEXO 1.1 Listado de Sitios para su integración de equipos

Juntas Electorales Distritales (CATD PREPET)						
No.	Municipio	Domicilio	Coordenada Geodésica	Total de Firewall UTM	Total de Switches	Total de Access Point
1	Cárdenas	Calle Caoba número 221 esq. Calle Ceiba, Fracc. Los Reyes Loma Alta, Cárdenas, Tabasco.	17.987398981484727, -93.39034505630875	1	1	2
2	Cárdenas	27 de febrero número 147, Col. Pueblo Nuevo, Cárdenas, Tabasco.	17.997224, -93.380146	1	1	2
3	Cárdenas	Calle Guadalupe Victoria esq. Venustiano Carranza s/n, Col. Centro, Cárdenas, Tabasco.	17.996722, -93.372699	1	1	2
4	Centla	Calle Benito Juárez Num. 406 Col. Centro, Frontera, Centla, Tabasco.	18.528326, -92.651923	1	1	2
5	Centro	Carretera a Ixtacomitán 1ra. Sección Km. 2.5 S/N Ra. Ixtacomitán 3a Sección, Villahermosa, Tabasco.	17.949185, -92.938595	1	1	2

No.	Municipio	Domicilio	Coordenada Geodésica	Total de Firewall UTM	Total de Switches	Total de Access Point
6	Centro	Calle Revolución No. 48 , Villa Maculteppec, C.P. 86250 Centro, Tabasco.	18.1390494, -92.8576822	1	1	2
7	Centro	Calle Sindicato de Economía Núm. 210, Col. Adolfo López Mateos, Villahermosa, Centro, Tabasco.	17.999580, -92.930194	1	1	2
8	Centro	Calle Alameda Núm. 8, Colonia Miguel Hidalgo, C.P. 86128 Villahermosa, Centro, Tabasco.	17.975474364818382, -92.97215775692511	1	1	2
9	Centro	C. Heroico Colegio Militar Núm. 125, Col. Primero de Mayo, C.P. 86100 Villahermosa, Tabasco.	17.978378, -92.942207	1	1	2
10	Centro	Calle Francisco I. Madero Núm. 202, Esquina Ausencio G. Cruz, Villa Playas del Rosario, Centro, Tabasco.	17.854460, -92.930267	1	1	2
11	Comalcalco	Calle Cacao Núm. 100, Col. las Rosas, Comalcalco, Tabasco.	18.257223, -93.212733	1	1	2
12	Comalcalco	Blvd. Leandro Rovirosa Wade Núm. 459, Colonia San Francisco C.P. 86330 Comalcalco, Tabasco.	18.269911, -93.226852	1	1	2
13	Cunduacán	Calle Playa del Rosario s/n, Fracc. Playa Azul, Col. Centro, Cunduacán; Tabasco.	18.062436, -93.173677	1	1	2
14	Emiliano Zapata	Calle Simón Sarlat Núm. 20, entre G. Méndez y Morelos , Col. Centro, E. Zapata, Tabasco.	17.743042, -91.764382	1	1	2
15	Huimanguillo	Av. De la Juventud Núm. 20, Col. Magisterial, Huimanguillo, Tabasco.	17.813667, -93.398661	1	1	2
16	Macuspana	Prol. Agustín Díaz del Castillo, Esq. Circunvalación, Macuspana, Tabasco.	17.753509, -92.588919	1	1	2
17	Jalpa de Méndez	Calle del Retén No. 4, Poblado Amatitán, Jalpa de Méndez, Tabasco.	18.1767943, -93.0804386	1	1	2
18	Nacajuca	Calle Crisanto Palma Núm 26, Col. Centro, Nacajuca, Tabasco.	18.16575793153521, -93.0181401729923	1	1	2
19	Paraíso	Calle Desiderio G. Rosado Sastré S/N, Col. Guanajai, C.P. 86607 Paraíso, Tabasco.	18.411712, -93.204267	1	1	2

20	Teapa	Av. Carlos A. Madrazo No. 190, Col. Sierra Arroyo, Teapa, Tabasco.	17.562814, -92.946193	1	1	2
21	Tenosique	C. Chichén Itzá S/N Fraccionamiento Pomona, Tenosique de Pino Suárez, Tabasco.	17.455857, -91.426581	1	1	2

Sitio principal Oficinas Centrales IEPCT						
No.	Municipio	Domicilio	Coordenada Geodésica	Total de Firewall UTM	Total de Switches	Total de Access Point
22	Centro	C. Eusebio Castillo 747, Nueva Villahermosa, 86000 Villahermosa, Tab.	17.994018835296785, -92.92081780739834	8	1	4

CCV (Centro de Captura y Verificación)						
No.	Municipio	Domicilio	Coordenada Geodésica	Total de Firewall UTM	Total de Switches	Total de Access Point
23	Centro	Av. Gregorio Méndez 716, Juan Álvarez y Eusebio Castillo, Fracc. Arboledas, Villahermosa, Centro, Tabasco	17.993233,-92.919256	2	2	2

Almacén General del IEPCT						
No.	Municipio	Domicilio	Coordenada Geodésica	Total de Firewall UTM	Total de Switches	Total de Access Point
24	Centro	Calle Revolución No. 605 B Colonia Tamulté de las Barrancas, CP 86150, Villahermosa, Tabasco.	17.9692164, -92.9552307	1	1	2
Edificio Sede Periférico (CATD para caso fortuito o fuerza mayor)						
25	Centro	Av. Periférico Carlos Pellicer Cámara No. 1206 Col. Tamulté de las Barrancas, Villahermosa, Tabasco	17.966291, -92.951558	1	1	2
Edificio Hidalgo						
26	Centro	Calle Hidalgo del 201 al 209, Colonia Centro, Villahermosa, Tabasco	17.988633939093567, -92.9203334	1	1	-

1. Características generales de la infraestructura de nube pública

1.1. El Proveedor de los Servicios deberá entregarlos desde un centro de datos que cumpla con al menos las siguientes certificaciones:

1.1.1. Certificación ISO/IEC 27001:2022 (Sistemas de gestión de seguridad de la información).

1.1.2. Certificación ISO/IEC 27017:2015 (Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube).

1.1.3. CSA STAR CCM v4.0 (Certificación nivel 2 de CSA STAR).

1.2. La infraestructura subyacente del proveedor deberá contar con alta disponibilidad y la escalabilidad y ancho de banda suficiente, que le permita disponer de los recursos cuando sea necesario.

1.3. Los servicios deberán contar con una infraestructura interna de red que permita en todo momento el funcionamiento óptimo. Entre otras cosas, deberá proveer:

1.3.1. Ancho de banda garantizado.
Los componentes que sean interconectados dentro de la nube, por ejemplo, la instancia de base de datos con los diferentes servidores deberá poder alcanzar hasta los 10 Gbps de velocidad de transferencia.

1.3.2. Zonas de Seguridad (CIDR's Públicos y Privados). El Proveedor de Servicios deberá contar con la infraestructura interna necesaria para permitir la creación de zonas de seguridad internas en base a subredes que aíslen los diferentes grupos de servicios, por ejemplo, el frontend (compuesto de servidores web) aislado de la capa de datos (compuesta por instancia de base de datos), o el sistema de capacitación del SIEE aislado del sistema de producción del SIEE, entre otros casos. Dichas zonas podrán ser Zonas Desmilitarizadas (DMZ) o similares.

1.3.3. Servicio de Resolución de Nombres. La infraestructura de nube deberá contar con Servicios de resolución de nombres (DNS) que se ajusten dinámicamente y de forma automática a la adición de nuevos Servicios, así como al crecimiento y/o reubicación de estos. El Servicio de resolución de nombres deberá tener una disponibilidad del 100%.

1.4. La solución de nube pública deberá estar presente en la sección de líderes del último reporte del Cuadrante Mágico de Gartner sobre infraestructura de nube pública.

2. Máquinas virtuales

2.1. Se requerirán instancias de máquinas virtuales con las siguientes características:

2.1.1. Dos máquinas virtuales con sistema operativo Windows Server Datacenter 2022 con licenciamiento incluido, almacenamiento de 80GB, 8 núcleos virtuales basados en el procesador AMD EPYC 7000 con velocidad de reloj turbo para todos los núcleos de hasta 2.5GHz o su equivalente en Intel, 32GB en RAM, interfaz de red de hasta 10Gbps de capacidad de transferencia de datos. Una máquina virtual se utilizará como servidor de Pruebas y Capacitación del SIEE y la segunda será el servidor de producción del SIEE.

2.1.2. Una máquina virtual con sistema operativo Ubuntu Server 22.04 LTS, almacenamiento de 80GB, 8 núcleos virtuales basados en el procesador AMD EPYC 7R13 con velocidad de reloj turbo para todos los núcleos de hasta 3.6GHz o su equivalente en Intel, 64GB en RAM, interfaz de red de hasta 10Gbps de capacidad de transferencia de datos. Se utilizará como servidor de PREP Casilla.

2.1.3. Dos máquinas virtuales con sistema operativo Ubuntu Server 22.04 LTS, almacenamiento de 80GB, 4 núcleos virtuales basados en el procesador AMD EPYC 7R13 con velocidad de reloj turbo para todos los núcleos de hasta 3.6GHz o su equivalente en Intel, 32GB en RAM, interfaz de red de hasta 10Gbps de capacidad de transferencia de datos. Una máquina virtual funcionará como servidor del sistema Conóceles y la segunda como servidor web de la página institucional.

2.1.4. Tres máquinas virtuales con sistema operativo Ubuntu Server 22.04 LTS, almacenamiento de 80GB, 36 núcleos virtuales basados en el procesador Intel Xeon Scalable de 2da generación (Cascade Lake 8223CL) o en un procesador Intel Xeon Platinum serie 8000 (Skylake 8124M) o su equivalente en AMD, 72GB en RAM, interfaz de red de hasta 10Gbps de capacidad de transferencia de datos. Las tres máquinas virtuales se utilizarán para el sistema PREPET.

2.1.5. Una máquina virtual con sistema operativo Ubuntu Server 22.04 LTS, almacenamiento de 500 GB, 4 núcleos virtuales basados en el procesador AMD EPYC 7000 con velocidad de reloj turbo para todos los núcleos de hasta 2.5GHz o su equivalente en Intel, 16GB en RAM, interfaz de red de hasta 10Gbps de capacidad de transferencia de datos. Esta máquina virtual se utilizará como servidor DNS.

2.2. Las instancias de máquinas virtuales deberán contar con al menos las siguientes características:

2.2.1. Capacidad para aumentar o disminuir la memoria RAM

2.2.2. Capacidad para aumentar o disminuir la cantidad de núcleos virtuales.

2.2.3. Capacidad para aumentar la capacidad de almacenamiento.

2.2.4. El almacenamiento de cada instancia debe ser basado en SSD, con al menos 500Mbps de capacidad de transferencia de datos.

2.2.5. Capacidad de autorrecuperación de la instancia causados por fallas del hardware o software (del host físico) subyacente.

2.2.6. Para que personal del IEPCT pueda instalar dentro de cada máquina virtual el software requerido de acuerdo con el rol que se pretenda con dicho servidor, se deberá permitir acceso mediante protocolo SSH a las máquinas virtuales con sistema operativo Linux y a los servidores con Windows Server mediante protocolo RDP, ambos con autenticación por llaves de seguridad, con permiso de administrador en cada instancia.

2.2.7. Para poder realizar su función ante la ciudadanía, las instancias deberán poder ser accedidas desde Internet a través de protocolo TCP o UDP.

3. Servicio de Balanceo.

Este Servicio tiene como función principal distribuir de forma automática el tráfico de red o flujos de operación que recibe el balanceador entre las máquinas virtuales que alojan los aplicativos y/o servicios, garantizando una distribución uniforme de la carga de trabajo de dichas máquinas virtuales.

3.1. Se requiere un servicio de balanceo de carga para distribuir y encaminar las peticiones al sistema PREPET entre los servidores mencionados en el punto **2.1.4**.

3.2. Características mínimas del Servicio:

3.2.1. La plataforma contará y operará con al menos alguno de los siguientes algoritmos de balanceo de tráfico, sin dejar fuera algún otro mecanismo de balanceo que cumpla con las funcionalidades mínimas aquí enlistadas:

3.2.1.1. Por utilización: Método de distribución de carga el cual toma en cuenta los niveles de utilización de la infraestructura que compone el Servicio, desbordando o desviando el flujo de tráfico hacia otra instancia o zona de manera automática, al momento de llegar al umbral de utilización previamente establecido.

3.2.1.2. Round Robin: Método de distribución de carga el cual asigna de manera equilibrada los flujos de comunicaciones entre las diversas instancias, tomando en cuenta el número de sesiones entrantes, dividido entre la cantidad de instancias disponibles.

3.2.2. Capacidad de operar bajo diferentes reglas de balanceo que se basen en los protocolos HTTP, HTTPS y TLS.

3.2.3. Enrutamiento automático por direccionamiento IP público o privado, con la capacidad de interactuar con Servicios de resolución de nombres DNS.

3.2.4. Balanceo entre Servicios Multi-Capas entre los diferentes Servicios de Nube pertenecientes al mismo proveedor.

3.2.5. El Servicio de balanceo deberá tener la capacidad y medios de acceso para poder ser administrado por el cliente si así lo decide, con el objetivo de obtener un auto aprovisionamiento de los recursos al momento de tener la necesidad de incrementar o disminuir los recursos cuando el IEPCT así lo requiera.

3.2.6. Contar con elasticidad automática.

4. Base de datos

El Servicio de Base de Datos deberá proveer todas las herramientas para su ejecución, así como los recursos de conectividad y administración necesarios para su correcto funcionamiento.

4.1. Características mínimas del servicio:

4.1.1. Soportar el manejador de base de datos MariaDB versión 10.5 o superior.

4.1.2. Contar con 8 núcleos virtuales basados en procesador Intel Xeon Platinum 8175 de 2.5 GHz o equivalente en AMD.

4.1.3. Contar con 32GB en RAM.

4.1.4. Capacidad de almacenamiento de 80GB, basado en SSD, con la posibilidad de crecimiento y que cuente con una tasa de transferencia de datos de al menos 500Mbps.

4.1.5. Rendimiento de interfaz de red de hasta 10Gbps.
4.1.6. Deberá incluir el licenciamiento correspondiente.
4.1.7. Contar con parámetros preconfigurados adecuados para cada tipo de instancia dedicada de base de datos definida por el IEPCT.
4.1.8. Asegurará el soporte y manejo de al menos los siguientes mecanismos de seguridad:
4.1.8.1. Cifrado de los datos en tránsito y en reposo de las Bases de Datos.
4.1.8.2. Manejo y soporte de mecanismos de control, autenticación, administración de privilegios de acceso a usuarios hacia los Servicios e información de las Bases de Datos.
4.1.8.3. Implementación de políticas en las que se deleguen funciones y accesos, así como desactivación de roles que no se requieran para el Servicio.
4.1.9. Contará con los mecanismos que permita agilizar y acelerar el despliegue del Servicio aquí descrito mediante automatización de la operación.
4.1.10. Contará con la capacidad y flexibilidad de crecimiento de manera casi inmediata, en el momento que el IEPCT así lo demande.
4.1.11. Deberá soportar y manejar mecanismos de seguridad para la instancia de base de datos, los cuales impidan los accesos que no hayan sido concedidos a través de las reglas del grupo de seguridad que defina el IEPCT.
4.2. Este Servicio deberá ser soportado y administrado desde la Consola de Administración de Servicios para asegurar la administración, aprovisionamiento de recursos asegurando un eficiente desempeño y rendimiento de los Servicios de Base de Datos.

5. Respaldos y restauración.

El proveedor del Servicio deberá garantizar la ejecución de respaldos automatizados, snapshots y en su caso la restauración del Servicio en caso de fallas o corrupción de datos.

5.1. La solución de respaldos debe contemplar los siguientes tipos:
5.1.1. Respaldo Total.
5.1.2. Respaldo Incremental.
5.2. Los servicios de respaldo se deberán aplicar a los siguientes recursos implementados:
5.2.1. Instancias de máquinas virtuales.
5.2.2. Instancias de bases de datos.
5.3. Se deberá generar un respaldo diario de cada recurso implementado, los cuales se deberán mantener por al menos 7 días.
5.4. Deberá contar con la capacidad de poder realizar respaldos manuales.
5.5.

6. Soporte técnico de la infraestructura de nube pública

Este Servicio considera actividades necesarias para la configuración, operación, optimización, mantenimiento proactivo y reactivo, soporte técnico y todo lo necesario para mantener en óptimo funcionamiento los componentes suministrados, debiendo cumplir al menos con lo siguiente:

6.1. Monitoreo de la infraestructura a través de la consola de Administración con acceso para el personal del IEPCT.
6.2. Borrado seguro de la información almacenada en los servicios de almacenamiento e instancias de cómputo.
6.3. Monitoreo y atención de las alertas generadas por los Servicios contratados.
6.4. Inventario detallado y actualizado de cada uno de los Servicios contratados.
6.5. Reporte de propuestas de optimización de los Servicios de Nube, que ayuden a las mejoras en el rendimiento de los mismos.
6.6. El Proveedor de Servicios debe contar con una mesa de Servicios para la atención de incidentes y requerimientos con una disponibilidad de atención de 5 días de la semana y 8 horas al día (5x8) y para las fechas de pruebas técnicas, simulacros y jornada electoral enunciadas en los puntos 6.7.1, .6.7.2 y 6.7.3,

se deberá contar con disponibilidad de atención de 24 horas. Para lo anterior se deberá cumplir al menos con las siguientes características.

6.6.1. El soporte deberá ser brindado vía email, chat, teléfono o acceso remoto.
6.6.2. La atención se deberá proporcionar en idioma español.
6.6.3. El soporte deberá incluir recomendaciones y mejores prácticas de seguridad de acuerdo resultados a la arquitectura de los Servicios del PREPET.

6.7. El proveedor de Servicios deberá suministrar personal para soporte en sitio de acuerdo con lo siguiente:
6.7.1. Un ingeniero de soporte por 8 horas durante cada prueba técnica en fechas 28 de abril y 5 de mayo del 2024.
6.7.2. Un ingeniero de soporte por 8 horas durante cada simulacro en fechas 12, 19 y 26 de mayo del 2024.
6.7.3. Un ingeniero de soporte disponible por 24 horas durante el día de la jornada electoral y fechas posteriores, correspondientes del 2 al 8 de junio de 2024. En caso de requerirse más tiempo, se contemplará asistencia remota hasta la culminación del contrato.

6.8. Indicadores y niveles de Servicio.
6.8.1. Indicador de Atención de Incidentes.
La tabla siguiente define los tiempos máximos esperados para las actividades de atención de incidentes, en función de la severidad del evento (los valores están expresados en minutos y horas hábiles, asimismo se solicita al proveedor proporcionar sus niveles de escalamiento acorde a estos niveles de Servicio que se solicitan):

- Para prioridad 1 (crítica), en donde el producto se encuentra inhabilitado y afecta críticamente el entorno productivo del IEPCT:
  - Tiempo de atención: <15minutos en modalidad 24x7
  - Tiempo de resolución estimado: 2 horas
- Para prioridad 2 (alta), en donde el producto está limitado en funcionalidad y el entorno productivo del IEPCT tiene afectación:
  - Tiempo de atención: <1 hora en modalidad 24x7
  - Tiempo de resolución estimado: 4 horas
- Para prioridad 3 (normal), en donde una funcionalidad específica del producto se ve afectada y el entorno productivo del IEPCT no tiene afectación:
  - Tiempo de atención: <2 horas en modalidad 24x7
  - Tiempo de resolución estimado: 16 horas
- Para prioridad 4 (baja), en el producto funciona adecuadamente y no hay afectación en el entorno productivo del IEPCT:
  - Tiempo de atención: <4 horas en modalidad 24x7
  - Tiempo de resolución estimado: 48 horas

Para las fechas en que solo se requiere soporte 8x5, los tiempos de respuesta para la Atención y Resolución Estimada se verán impactados por el fin de la jornada laboral. En cuyo caso, se le seguirá dando atención en el siguiente día hábil.

6.9. Niveles de Servicio

Los niveles de Servicio solicitados y que deberán ser reportados en línea con corte mensual. Así como los reportes requeridos del Servicio se presentan a continuación:

- Disponibilidad mensual del balanceador de carga >= 99.99%
- Disponibilidad mensual del servicio de monitoreo de los recursos implementados en la nube >= 99.9%
- Disponibilidad mensual de instancias de máquinas virtuales >= 99.5%
- Disponibilidad mensual de instancias de base de datos >= 99.95%

6.10. Entregables

Como parte de la entrega del servicio el proveedor deberá proporcionar al IEPCT los siguientes entregables, los cuales se consideran de manera enunciativa, más no limitativa, durante la vigencia del Servicio, los reportes listados podrán sufrir cambios:

- La carta compromiso del Licitante del nivel de disponibilidad de los Servicios se deberá entregar como parte de la propuesta.
- Los reportes de monitoreo de CPU, de memoria, de almacenamiento, se deberán entregar 5 días hábiles previos a la finalización del contrato.
- Los reportes de incidentes ocurridos durante la vigencia del contrato se deberán entregar 5 días hábiles posteriores a la finalización del contrato.
- El documento con la relación de las credenciales de acceso se deberá entregar 3 días hábiles posteriores a la fecha de inicio del Servicio.
- El Plan de trabajo inicial se deberá entregar 10 días hábiles posteriores a la fecha de adjudicación.

6.11. El Proveedor del Servicio deberá entregar en los tiempos que Indique el IEPCT todos los elementos técnicos, documentales, medios de respaldo, etc. que le sean requeridos para mover sus aplicaciones y datos a otra Infraestructura. Al término del contrato, el Proveedor del Servicio, deberá facilitar la transferencia de toda la información de las aplicaciones en la Nube hacia la infraestructura que el IEPCT indique.

6.12. El IEPCT notificará al Proveedor cuando considere que los recursos implementados en la nube han superado las pruebas pertinentes y la solución funciona según lo previsto. El IEPCT ya no realizará modificaciones a la solución. El Proveedor debe implementar los recursos en la nube necesarios para que la solución funcione en alta disponibilidad (activo-pasivo) para las instancias de máquinas virtuales, la base de datos y el balanceador de carga.

7. Transferencia de conocimientos de la infraestructura de nube pública

El Servicio de transferencia de conocimientos, deberá contar con al menos las siguientes características:

7.1. El proveedor de Servicios deberá considerar la Transferencia de Conocimientos (presencial y/o a distancia) en el uso de todos los componentes requeridos.

7.2. El Servicio de transferencia de conocimiento se deberá realizar para al menos 10 personas.

8. Ciberseguridad

Se deberán integrar en la propuesta, equipos físicos para la seguridad perimetral de las Juntas Distritales y Oficina Central y soluciones virtuales para la protección de la infraestructura de nube pública y la administración de todos los elementos de ciberseguridad.

8.1. **30 equipos Firewall UTM (Administración Unificada de Amenazas)** la cuales estarán distribuidos de la siguiente manera: **21** para las Juntas Electorales Distritales (CATD), **1** para el Almacén General, **1** para el Edificio Sede Periférico, **1** para el Edificio de Hidalgo y **6** equipos disponibles de respaldo de caso fortuito que serán entregados en puntos estratégicos para cualquier situación de falla de algún equipo.

8.1.1. Características del dispositivo:

8.1.1.1. El dispositivo debe ser un "appliance" de propósito específico "Hardware"

8.1.1.2. Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.

8.1.1.3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
8.1.1.4. Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
8.1.1.5. El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.
8.1.1.6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
8.1.1.7. A excepción de la funcionalidad de VPN's, todas las demás funcionalidades en modo Gateway deben estar presentes en modo transparente.
8.1.1.8. La herramienta deberá de funcionar desde un inicio como Modo Gateway, Modo Transparente y Modo Proxy explícito.

8.1.2. Características del Sistema operativo incluido:
8.1.2.1. Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows.
8.1.2.2. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.
8.1.3. Firewall
8.1.3.1. Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
8.1.3.2. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
8.1.3.3. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
8.1.3.4. Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
8.1.3.5. Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.
8.1.3.6. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación.
8.1.3.7. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
8.1.3.8. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
8.1.3.9. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
8.1.3.10. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
8.1.3.11. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP).
8.1.3.12. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
8.1.3.13. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
8.1.3.14. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
8.1.3.15. La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.

8.1.3.16. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID

8.1.3.17. En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.

8.1.3.18. La solución deberá tener la capacidad de procesamiento para orquestar la red completa a través de tecnologías de fábrica seguro donde se pueda gestionar, si así se requiere switches de capa 2 y puntos de acceso inalámbrico, con los que podrá interactuar y configurar de manera puntual desde la misma interfaz gráfica del firewall.
Deberá ser capaz de usar conectores de Software (REST API) que permitan disparar mecanismos de contención en caso de un ataque a nivel de acceso ya sea en los switches y o en los puntos de acceso de la misma solución para aislar cualquier ataque que pudieran darse a nivel de capa 2.

8.1.4. Conectividad y Sistema de ruteo

8.1.4.1. Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.

8.1.4.2. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.

8.1.4.3. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.

8.1.4.4. Soporte a políticas de ruteo (policy routing).

8.1.4.5. El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.

8.1.4.6. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.

8.1.4.7. Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+.

8.1.4.8. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.

8.1.4.9. Soporte de ECMP (Equal Cost Multi-Path).

8.1.4.10. Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.

8.1.4.11. Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.

8.1.4.12. Soporte a ruteo de multicast.

8.1.4.13. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

8.1.4.14. La solución deberá incluir de manera nativa tecnologías de redes de área amplia definida por software, también conocida por siglas en inglés como SD-WAN, esto con la finalidad de agilizar las operaciones y garantizar iniciativas de transformación digital. Reducir complejidad de administración de enlaces hacia internet, mejorar la experiencia de las aplicaciones, ahorrar costos de enlaces demasiados costosos y tener un solo punto de administración y monitoreo de los enlaces.

8.1.4.15. Estas tecnologías deberán soportar varios tipos de enlaces tales como enlaces simétricos, asimétricos, ADSL, 3G/4LTE unificarlos y poder crear interfaces virtuales de salida hacia wan unificando estas clases de tecnologías WAN.

8.1.4.16. Así también permitirá monitorear las interfaces virtuales basado en volumen y sesiones y mostrar en tiempo real el comportamiento de las interfaces virtuales.

8.1.4.17. De manera nativa deberá soportar de igual forma seguridad embebida para el tráfico entrante o saliente a través de las interfaces virtuales.

8.1.4.18. Deberá permitir reconocer y dar prioridad basado en volumen, sesiones, calidad de enlace y cantidad de tráfico.

8.1.5. VPN IPSec/L2TP/PPTP

8.1.5.1. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).

8.1.5.2. Soporte para IKEv2 y IKE Configuration Method.
8.1.5.3. Debe soportar la configuración de túneles L2TP.
8.1.5.4. Debe soportar la configuración de túneles PPTP.
8.1.5.5. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
8.1.5.6. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
8.1.5.7. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
8.1.5.8. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
8.1.5.9. Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
8.1.5.10. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
8.1.5.11. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
8.1.5.12. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

8.1.6. VPN SSL
8.1.6.1. Capacidad de realizar SSL VPNs.
8.1.6.2. Soporte a certificados PKI X.509 para construcción de VPNs SSL.
8.1.6.3. Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
8.1.6.4. Soporte de renovación de contraseñas para LDAP y RADIUS.
8.1.6.5. Soporte a asignación de aplicaciones permitidas por grupo de usuarios
8.1.6.6. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
8.1.6.7. Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
8.1.6.8. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).
8.1.6.9. La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS.
8.1.6.10. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL.
8.1.6.11. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
8.1.6.12. Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
8.1.6.13. Los portales personalizados deberán soportar al menos la definición de:
- Widgets a mostrar.
- Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
- Esquema de colores.
- Soporte para Escritorio Virtual.
- Política de verificación de la estación de trabajo.

8.1.6.14. La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
8.1.6.15. En la configuración del Escritorio Virtual podrá definirse como mínimo:
- La posibilidad de que el usuario cambie entre escritorio virtual y real.
- La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.
- La posibilidad de utilizar medios removibles desde el escritorio virtual.
- La posibilidad de acceder a recursos compartidos desde el escritorio virtual.

- La posibilidad de imprimir desde el escritorio virtual.
- La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.

8.1.7. Traffic Shapping / QoS

8.1.7.1. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.

8.1.7.2. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.

8.1.7.3. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

8.1.7.4. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.

8.1.7.5. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo.

8.1.7.6. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.

8.1.8. Autenticación y Certificación Digital.

8.1.8.1. Capacidad de integrarse con Servidores de Autenticación RADIUS.

8.1.8.2. Capacidad nativa de integrarse con directorios LDAP.

8.1.8.3. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".

8.1.8.4. Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.

8.1.8.5. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.

8.1.8.6. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).

8.1.8.7. Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.

8.1.8.8. Soporte de verificación de validación de certificados digitales mediante el protocolo OSCP (Online Simple Enrrollment Protocol).

8.1.8.9. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.

8.1.8.10. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.

8.1.8.11. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:

- Longitud mínima permitida.
- Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
- Expiración de contraseña.

8.1.8.12. Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

8.1.9. Protección contra intrusos (IPS)

8.1.9.1. El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en SPAN o MIRROR.

8.1.9.2. El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.

8.1.9.3. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.

8.1.9.4. Capacidad de detección de más de 4,000 ataques.

8.1.9.5. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin

programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).

8.1.9.6. El detector y preventor de intrusos deberá de estar orientado para la protección de redes.

8.1.9.7. El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.

8.1.9.8. El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).

8.1.9.9. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.

8.1.9.10. Tecnología de detección tipo Stateful basada en Firmas (signatures).

8.1.9.11. Actualización automática de firmas para el detector de intrusos.

8.1.9.12. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.

8.1.9.13. "Mecanismos de detección de ataques:

- Reconocimiento de patrones y Análisis de protocolos.
- Detección de anomalías.
- Detección de ataques de RPC (Remote procedure call).
- Protección contra ataques de Windows o NetBios.
- Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)
- Protección contra ataques DNS (Domain Name System)
- Protección contra ataques a FTP, SSH , Telnet y Rlogin
- Protección contra ataques de ICMP (Internet Control Message Protocol)."

8.1.9.14. "Métodos de notificación:

8.1.9.15. Alarmas mostradas en la consola de administración del "appliance".

- Alertas vía correo electrónico.
- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto."
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

8.1.10. Prevención de Fuga de Información (DLP)

8.1.10.1. La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.

8.1.10.2. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.

8.1.10.3. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.

8.1.10.4. Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.

8.1.10.5. En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
8.1.10.6. La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
8.1.10.7. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

8.1.11. Control de Aplicaciones
8.1.11.1. La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
8.1.11.2. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
8.1.11.3. La solución debe tener un listado de al menos 3,000 aplicaciones ya definidas por el fabricante.
8.1.11.4. El listado de aplicaciones debe actualizarse periódicamente.
8.1.11.5. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
8.1.11.6. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
8.1.11.7. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
8.1.11.8. Preferentemente deben soportar mayor granularidad en las acciones.

8.1.12. Inspección de Contenido SSL
8.1.12.1. La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
8.1.12.2. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
8.1.12.3. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
8.1.12.4. Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.

8.1.13. Antivirus
8.1.13.1. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
8.1.13.2. El Antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.
8.1.13.3. Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
8.1.13.4. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
8.1.13.5. La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo "appliance", que permita la aplicación de esta protección por política de control de acceso.

8.1.13.6. El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
8.1.13.7. El "appliance" deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List).
8.1.13.8. El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos Http, FTP, IMAP, POP3, SMTP.
8.1.13.9. El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
8.1.13.10. El Antivirus deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.
8.1.13.11. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
8.1.13.12. El antivirus deberá ser capaz de filtrar archivos por extensión.
8.1.13.13. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tenga el archivo.
8.1.13.14. Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
8.1.13.15. Las firmas de antivirus deberán ser del mismo fabricante que el "appliance".
8.1.13.16. El sistema debe ser capaz de integrarse a futuro con una solución de sanboxing del mismo fabricante de manera que se pueda aprovechar las firmas generadas en el Firewall.

8.1.14. AntiSpam
8.1.14.1. La capacidad AntiSpam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
8.1.14.2. La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
8.1.14.3. La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM.
8.1.14.4. En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

8.1.15. Filtrado de URLs (URL Filtering)
8.1.15.1. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
8.1.15.2. Debe poder categorizar contenido Web requerido mediante IPv6.
8.1.15.3. Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
8.1.15.4. Configurable directamente desde la interfaz de administración del dispositivo "appliance". Con capacidad para permitir esta protección por política de control de acceso.

8.1.15.5. Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
8.1.15.6. Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
8.1.15.7. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
8.1.15.8. La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing.
8.1.15.9. La solución deberá de ser capaz de poder bloquear el acceso cuentas de dominios específicos a servicios de Google como por ejemplo GMail, Gdocs.
8.1.15.10. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
8.1.15.11. Será posible exceptuar la inspección de HTTPS por categoría.

8.1.16. Alta Disponibilidad
8.1.16.1. Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.
8.1.16.2. Alta Disponibilidad en modo Activo-Pasivo.
8.1.16.3. Alta Disponibilidad en modo Activo-Activo.
8.1.16.4. Posibilidad de definir al menos dos interfaces para sincronía.
8.1.16.5. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.
8.1.16.6. Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.
8.1.17. Características de Administración
8.1.17.1. Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
8.1.17.2. La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.
8.1.17.3. Interfaz basada en línea de comando (CLI) para administración de la solución.
8.1.17.4. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
8.1.17.5. Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
8.1.17.6. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
8.1.17.7. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
8.1.17.8. El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.
8.1.17.9. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
8.1.17.10. Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
8.1.17.11. Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.

8.1.17.12. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.
8.1.17.13. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
8.1.17.14. Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
8.1.17.15. Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.

8.1.18. Virtualización
8.1.18.1. El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
8.1.18.2. La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
8.1.18.3. Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.
8.1.18.4. Cada instancia virtual debe poder tener un administrador independiente
8.1.18.5. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
8.1.18.6. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
8.1.18.7. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
8.1.18.8. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
8.1.18.9. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

8.1.19. Licenciamiento, Soporte y Actualizaciones
8.1.19.1. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios y conexiones limitándola solamente por el desempeño del equipo.
8.1.19.2. La vigencia de licencia de actualización debe incluirse la capacidad de poder hacer actualizaciones de firmas IPS, URL Filtering, antispam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo con las características arriba descritas, por espacio mínimo de 1 año.
8.1.19.3. La solución debe contar con un Centro de Investigación propio del mismo fabricante para la actualización de políticas
8.1.19.4. El equipo debe de incluir Soporte Telefónica, Reemplazo de Fábrica, Actualizaciones de Firmware por al menos 1 año.
8.1.19.5. El fabricante deberá contar con un centro de atención al cliente (TAC) basado en la ciudad de México con atención y soporte en lenguaje Inglés y Español. Además de un soporte mundial tipo "follow-the-sun".

8.1.20. Capacidades de desempeño
- El equipo debe contar con un Throughput Firewall de al menos 10 Gbps para paquetes de 512 bytes de UDP y 6 Gigabytes para para paquetes de 64 bytes, el desempeño de Firewall aplica tanto para tráfico IPv4 como IPv6.
- El equipo debe contar con un Throughput VPN IPSec de por lo menos 6.5 Gbps.
- El equipo debe contar con un Throughput VPN SSL de por lo menos 750 Mbps.
- El equipo debe contar con un Throughput IPS de al menos 1.4 Gbps para web.
- El equipo debe contar con un Throughput de Firewall de Nueva Generación (NGFW) de al menos 1 Gbps.
- El equipo debe contar con un Throughput de inspección de tráfico SSL de por lo menos 750 Mbps.

- El equipo debe contar con al menos 700 mil Sesiones concurrentes.
- El equipo debe soportar al menos 35,000 Nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo debe poder generar al menos 500 VPN's IPSec Client to Gateway y 200 VPN's IPSec Gateway to Gateway.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 10 virtual Firewalls.
- De igual forma el desempeño en next generation firewall mode de al menos 1 Gb/s
- Desempeño en firewall de aplicaciones de al menos 1.8 Gb/s
- Características de Hardware:
- El equipo debe contar con al menos 7 Interfaces GigaEthernet RJ45.
- El equipo debe contar con al menos 2 interfaces GigaEthernet exclusiva para WAN.

8.2. **2 equipos Firewall UTM (Administración Unificada de Amenazas)** en configuración de alta disponibilidad para el Centro de Captura y Verificación con las siguientes:

8.2.1. Características del dispositivo

8.2.1.1. El dispositivo debe ser un "appliance" de propósito específico "Hardware"

8.2.1.2. Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.

8.2.1.3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).

8.2.1.4. Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).

8.2.1.5. El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.

8.2.1.6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

8.2.1.7. A excepción de la funcionalidad de VPN's, todas las demás funcionalidades en modo Gateway deben estar presentes en modo transparente.

8.2.1.8. La herramienta deberá de funcionar desde un inicio como Modo Gateway, Modo Transparente y Modo Proxy explícito.

8.2.2. Características del Sistema operativo incluido

8.2.2.1. Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows

8.2.2.2. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas, de acuerdo a la configuración del administrador.

8.2.3. Firewall

8.2.3.1. Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs

8.2.3.2. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.

8.2.3.3. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.

8.2.3.4. Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
8.2.3.5. Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.
8.2.3.6. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
8.2.3.7. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
8.2.3.8. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
8.2.3.9. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
8.2.3.10. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
8.2.3.11. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
8.2.3.12. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
8.2.3.13. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
8.2.3.14. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)
8.2.3.15. La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas
8.2.3.16. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
8.2.3.17. En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
8.2.3.18. La solución deberá tener la capacidad de procesamiento para orquestar la red completa a través de tecnologías de malla seguro donde se pueda gestionar, si así se requiere switches de capa 2 y puntos de acceso inalámbrico, con los que podrá interactuar y configurar de manera puntual desde la misma interfaz gráfica del firewall.
8.2.3.19. Deberá ser capaz de usar conectores de Software (REST API) que permitan disparar mecanismos de contención en caso de un ataque a nivel de acceso ya sea en los switches y o en los puntos de acceso de la misma solución para aislar cualquier ataque que pudieran darse a nivel de capa 2.

8.2.4. Conectividad y Sistema de ruteo
8.2.4.1. Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
8.2.4.2. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
8.2.4.3. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
8.2.4.4. Soporte a políticas de ruteo (policy routing)
8.2.4.5. El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.
8.2.4.6. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.
8.2.4.7. Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+
8.2.4.8. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
8.2.4.9. Soporte de ECMP (Equal Cost Multi-Path)
8.2.4.10. Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.

8.2.4.11. Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.

8.2.4.12. Soporte a ruteo de multicast

8.2.4.13. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

8.2.4.14. La solución deberá incluir de manera nativa tecnologías de redes de área amplia definida por software, también conocida por siglas en inglés como SD-WAN, esto con la finalidad de agilizar las operaciones y garantizar iniciativas de transformación digital. Reducir complejidad de administración de enlaces hacia internet, mejorar la experiencia de las aplicaciones, ahorrar costos de enlaces demasiados costosos y tener una sola punto de administración y monitoreo de los enlaces.

8.2.4.15. Estas tecnologías deberán soportar varios tipos de enlaces tales como enlaces simétricos, asimétricos, ADSL, 3G/4LTE unificarlos y poder crear interfaces virtuales de salida hacia wan unificando estas clases de tecnologías WAN.

8.2.4.16. Así también permitirá monitorear las interfaces virtuales basado en volumen y sesiones y mostrar en tiempo real el comportamiento de las interfaces virtuales.

8.2.4.17. De manera nativa deberá soportar de igual forma seguridad embebida para el trafico entrante o saliente a través de las interfaces virtuales.

8.2.4.18. Deberá permitir reconocer y dar prioridad basado en volumen, sesiones, calidad de enlace y cantidad de tráfico.

8.2.5. VPN IPSec/L2TP/PPTP

8.2.5.1. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).

8.2.5.2. Soporte para IKEv2 y IKE Configuration Method.

8.2.5.3. Debe soportar la configuración de túneles L2TP.

8.2.5.4. Debe soportar la configuración de túneles PPTP.

8.2.5.5. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.

8.2.5.6. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.

8.2.5.7. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.

8.2.5.8. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.

8.2.5.9. Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.

8.2.5.10. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).

8.2.5.11. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.

8.2.5.12. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

8.2.6. VPN SSL

8.2.6.1. Capacidad de realizar SSL VPNs.

8.2.6.2. Soporte a certificados PKI X.509 para construcción de VPNs SSL.

8.2.6.3. Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.

8.2.6.4. Soporte de renovación de contraseñas para LDAP y RADIUS.

8.2.6.5. Soporte a asignación de aplicaciones permitidas por grupo de usuarios

8.2.6.6. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.

8.2.6.7. Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.

8.2.6.8. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)

8.2.6.9. La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS

8.2.6.10. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL

8.2.6.11. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente

8.2.6.12. Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.

8.2.6.13. Los portales personalizados deberán soportar al menos la definición de:

- Widgets a mostrar.
- Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
- Esquema de colores.
- Soporte para Escritorio Virtual.
- Política de verificación de la estación de trabajo.

8.2.6.14. La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.

8.2.6.15. En la configuración del Escritorio Virtual podrá definirse como mínimo:

- La posibilidad de que el usuario cambie entre escritorio virtual y real.
- La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.
- La posibilidad de utilizar medios removibles desde el escritorio virtual.
- La posibilidad de acceder a recursos compartidos desde el escritorio virtual.
- La posibilidad de imprimir desde el escritorio virtual.
- La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.

8.2.7. Traffic Shapping / QoS

8.2.7.1. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.

8.2.7.2. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.

8.2.7.3. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

8.2.7.4. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.

8.2.7.5. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo

8.2.7.6. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.

8.2.8. Autenticación y Certificación Digital.

8.2.8.1. Capacidad de integrarse con Servidores de Autenticación RADIUS.

8.2.8.2. Capacidad nativa de integrarse con directorios LDAP.

8.2.8.3. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".

8.2.8.4. Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.

8.2.8.5. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.

8.2.8.6. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).

8.2.8.7. Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.

8.2.8.8. Soporte de verificación de validación de certificados digitales mediante el protocolo OSCP (Online Simple Enrrollment Protocol).
8.2.8.9. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
8.2.8.10. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
8.2.8.11. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
- Longitud mínima permitida.
- Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
- Expiración de contraseña.

8.2.8.12. Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

8.2.9. Protección contra intrusos (IPS)
8.2.9.1. El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en SPAN o MIRROR.
8.2.9.2. El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.
8.2.9.3. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.
8.2.9.4. Capacidad de detección de más de 4,000 ataques.
8.2.9.5. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
8.2.9.6. El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.
8.2.9.7. El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
8.2.9.8. El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).
8.2.9.9. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
8.2.9.10. Tecnología de detección tipo Stateful basada en Firmas (signatures).
8.2.9.11. Actualización automática de firmas para el detector de intrusos.
8.2.9.12. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
8.2.9.13. Mecanismos de detección de ataques:
- Reconocimiento de patrones y Análisis de protocolos.
- Detección de anomalías.
- Detección de ataques de RPC (Remote procedure call).
- Protección contra ataques de Windows o NetBios.
- Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)
- Protección contra ataques DNS (Domain Name System)
- Protección contra ataques a FTP, SSH , Telnet y Rlogin
- Protección contra ataques de ICMP (Internet Control Message Protocol)."

8.2.9.14. "Métodos de notificación:
8.2.9.15. Alarmas mostradas en la consola de administración del "appliance".

- Alertas vía correo electrónico.
- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto."
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

8.2.10. Prevención de Fuga de Información (DLP)
8.2.10.1. La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
8.2.10.2. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
8.2.10.3. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
8.2.10.4. Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.
8.2.10.5. En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
8.2.10.6. La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
8.2.10.7. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
8.2.11. Control de Aplicaciones
8.2.11.1. La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
8.2.11.2. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
8.2.11.3. La solución debe tener un listado de al menos 3,000 aplicaciones ya definidas por el fabricante.
8.2.11.4. El listado de aplicaciones debe actualizarse periódicamente.
8.2.11.5. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
8.2.11.6. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
8.2.11.7. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
8.2.11.8. Preferentemente deben soportar mayor granularidad en las acciones.
8.2.12. Inspección de Contenido SSL
8.2.12.1. La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
8.2.12.2. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
8.2.12.3. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

8.2.12.4. Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.

8.2.13. Antivirus

8.2.13.1. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.

8.2.13.2. El Antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.

8.2.13.3. Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.

8.2.13.4. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.

8.2.13.5. La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo "appliance", que permita la aplicación de esta protección por política de control de acceso.

8.2.13.6. El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.

8.2.13.7. El "appliance" deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List).

8.2.13.8. El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos Http, FTP, IMAP, POP3, SMTP.

8.2.13.9. El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.

8.2.13.10. El Antivirus deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.

8.2.13.11. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).

8.2.13.12. El antivirus deberá ser capaz de filtrar archivos por extensión.

8.2.13.13. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tenga el archivo.

8.2.13.14. Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).

8.2.13.15. Las firmas de antivirus deberán ser del mismo fabricante que el "appliance".

8.2.13.16. El sistema debe ser capaz de integrarse a futuro con una solución de sanboxing del mismo fabricante de manera que se pueda aprovechar las firmas generadas en el Firewall.

8.2.14. AntiSpam

8.2.14.1. La capacidad AntiSpam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.

8.2.14.2. La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).

8.2.14.3. La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM.

8.2.14.4. En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

8.2.15. Filtrado de URLs (URL Filtering)

8.2.15.1. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.

8.2.15.2. Debe poder categorizar contenido Web requerido mediante IPv6.

8.2.15.3. Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.

8.2.15.4. Configurable directamente desde la interfaz de administración del dispositivo "appliance". Con capacidad para permitir esta protección por política de control de acceso.

8.2.15.5. Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.

8.2.15.6. Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.

8.2.15.7. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).

8.2.15.8. La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing.

8.2.15.9. La solución deberá de ser capaz de poder bloquear el acceso cuentas de dominios específicos a servicios de Google como por ejemplo GMail, Gdocs.

8.2.15.10. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.

8.2.15.11. Será posible exceptuar la inspección de HTTPS por categoría.

8.2.16. Alta Disponibilidad

8.2.16.1. Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.

8.2.16.2. Alta Disponibilidad en modo Activo-Pasivo.

8.2.16.3. Alta Disponibilidad en modo Activo-Activo.

8.2.16.4. Posibilidad de definir al menos dos interfaces para sincronía.

8.2.16.5. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.

8.2.16.6. Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.

8.2.17. Características de Administración

8.2.17.1. Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).

8.2.17.2. La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.

8.2.17.3. Interfaz basada en línea de comando (CLI) para administración de la solución.
8.2.17.4. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
8.2.17.5. Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
8.2.17.6. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
8.2.17.7. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
8.2.17.8. El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.
8.2.17.9. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
8.2.17.10. Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
8.2.17.11. Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.
8.2.17.12. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.
8.2.17.13. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
8.2.17.14. Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
8.2.17.15. Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.

8.2.18. Virtualización
8.2.18.1. El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
8.2.18.2. La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
8.2.18.3. Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.
8.2.18.4. Cada instancia virtual debe poder tener un administrador independiente
8.2.18.5. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
8.2.18.6. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
8.2.18.7. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
8.2.18.8. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
8.2.18.9. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

8.2.19. Licenciamiento, Soporte y Actualizaciones
8.2.19.1. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios y conexiones limitándola solamente por el desempeño del equipo.
8.2.19.2. La vigencia de licencia de actualización debe incluirse la capacidad de poder hacer actualizaciones de firmas IPS, URL Filtering, antispam, antivirus y cualquier otra actualización

necesaria para la correcta operación del equipo con las características arriba descritas, por espacio mínimo de 1 año.

8.2.19.3. La solución debe contar con un Centro de Investigación propio del mismo fabricante para la actualización de políticas.

8.2.19.4. El equipo debe de incluir Soporte Telefónica, Reemplazo de Fábrica, Actualizaciones de Firmware por 1 año.

8.2.19.5. El fabricante deberá contar con un centro de atención al cliente (TAC) basado en la ciudad de México con atención y soporte en lenguaje inglés y español. Además de un soporte mundial tipo "follow-the-sun".

8.2.20. Capacidades de desempeño

- El equipo debe contar con un Throughput Firewall de al menos 9 Gbps para paquetes de 512 bytes de UDP y 6 Gigabytes para para paquetes de 64 bytes, el desempeño de Firewall aplica tanto para tráfico IPv4 como IPv6.
- El equipo debe contar con un Throughput VPN IPSec de por lo menos 6 Gbps.
- El equipo debe contar con un Throughput VPN SSL de por lo menos 950 Mbps.
- El equipo debe contar con un Throughput IPS de al menos 1.2 Gbps para web.
- El equipo debe contar con un Throughput de Firewall de Nueva Generación (NGFW) de al menos 1 Gbps.
- El equipo debe contar con un Throughput de inspección de tráfico SSL de por lo menos 700 Mbps.
- El equipo debe contar con al menos 1.2 millones de Sesiones concurrentes.
- El equipo debe soportar al menos 40,000 Nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo debe poder generar al menos 2500 VPN's IPSec Client to Gateway y 200 VPN's IPSec Gateway to Gateway.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 10 virtual Firewalls.
- De igual forma el desempeño en next generation firewall mode de al menos 1 Gb/s
- Desempeño en firewall de aplicaciones de al menos 1.8 Gb/s
- El equipo debe contar con al menos 6 Interfaces GigaEthernet RJ45 aceleradas por hardware y 2 puertos ethernet SPF
- El equipo debe contar una fuente de poder redundante para N+1

8.3. **Dos equipos Firewall UTM (Administración Unificada de Amenazas)** en configuración de alta disponibilidad para la oficina central del IEPCT con las siguientes:

8.3.1. Características del dispositivo:

8.3.1.1. El dispositivo debe ser un "appliance" de propósito específico "Hardware"

8.3.1.2. Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.

8.3.1.3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).

8.3.1.4. Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).

8.3.1.5. El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.

8.3.1.6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
8.3.1.7. A excepción de la funcionalidad de VPN's, todas las demás funcionalidades en modo Gateway deben estar presentes en modo transparente.
8.3.1.8. La herramienta deberá de funcionar desde un inicio como Modo Gateway, Modo Transparente y Modo Proxy explícito.

8.3.2. Características del Sistema operativo incluido
8.3.2.1. Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
8.3.2.2. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

8.3.3. Firewall
8.3.3.1. Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
8.3.3.2. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
8.3.3.3. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
8.3.3.4. Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
8.3.3.5. Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.
8.3.3.6. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación.
8.3.3.7. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
8.3.3.8. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
8.3.3.9. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
8.3.3.10. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
8.3.3.11. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
8.3.3.12. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
8.3.3.13. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
8.3.3.14. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
8.3.3.15. La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
8.3.3.16. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session I
8.3.3.17. En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
8.3.3.18. La solución deberá tener la capacidad de procesamiento para orquestar la red completa a través de tecnologías de malla seguro donde se pueda gestionar, si así se requiere switches de

capa 2 y puntos de acceso inalámbrico, con los que podrá interactuar y configurar de manera puntual desde la misma interfaz gráfica del firewall.

8.3.3.19. Deberá ser capaz de usar conectores de Software (REST API) que permitan disparar mecanismos de contención en caso de un ataque a nivel de acceso ya sea en los switches y o en los puntos de acceso de la misma solución para aislar cualquier ataque que pudieran darse a nivel de capa 2.

8.3.4. Conectividad y Sistema de ruteo

8.3.4.1. Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.

8.3.4.2. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.

8.3.4.3. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.

8.3.4.4. Soporte a políticas de ruteo (policy routing)

8.3.4.5. El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.

8.3.4.6. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.

8.3.4.7. Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+

8.3.4.8. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.

8.3.4.9. Soporte de ECMP (Equal Cost Multi-Path)

8.3.4.10. Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.

8.3.4.11. Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.

8.3.4.12. Soporte a ruteo de multicast

8.3.4.13. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

8.3.4.14. La solución deberá incluir de manera nativa tecnologías de redes de área amplia definida por software, también conocida por siglas en inglés como SD-WAN, esto con la finalidad de agilizar las operaciones y garantizar iniciativas de transformación digital. Reducir complejidad de administración de enlaces hacia internet, mejorar la experiencia de las aplicaciones, ahorrar costos de enlaces demasiados costosos y tener una sola punto de administración y monitoreo de los enlaces.

8.3.4.15. Estas tecnologías deberán soportar varios tipos de enlaces tales como enlaces simétricos, asimétricos, ADSL, 3G/4LTE unificarlos y poder crear interfaces virtuales de salida hacia wan unificando estas clases de tecnologías WAN.

8.3.4.16. Así también permitirá monitorear las interfaces virtuales basado en volumen y sesiones y mostrar en tiempo real el comportamiento de las interfaces virtuales.

8.3.4.17. De manera nativa deberá soportar de igual forma seguridad embebida para el trafico entrante o saliente a través de las interfaces virtuales.

8.3.4.18. Deberá permitir reconocer y dar prioridad basado en volumen, sesiones, calidad de enlace y cantidad de tráfico.

8.3.5. VPN IPSec/L2TP/PPTP

8.3.5.1. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).

8.3.5.2. Soporte para IKEv2 y IKE Configuration Method.

8.3.5.3. Debe soportar la configuración de túneles L2TP.

8.3.5.4. Debe soportar la configuración de túneles PPTP.

8.3.5.5. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.

8.3.5.6. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.

8.3.5.7. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.

8.3.5.8. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.

8.3.5.9. Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.

8.3.5.10. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
8.3.5.11. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
8.3.5.12. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X

8.3.6. VPN SSL
8.3.6.1. Capacidad de realizar SSL VPNs.
8.3.6.2. Soporte a certificados PKI X.509 para construcción de VPNs SSL.
8.3.6.3. Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
8.3.6.4. Soporte de renovación de contraseñas para LDAP y RADIUS.
8.3.6.5. Soporte a asignación de aplicaciones permitidas por grupo de usuarios
8.3.6.6. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
8.3.6.7. Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
8.3.6.8. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)
8.3.6.9. La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS
8.3.6.10. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
8.3.6.11. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
8.3.6.12. Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
8.3.6.13. Los portales personalizados deberán soportar al menos la definición de:
- Widgets a mostrar.
- Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
- Esquema de colores.
- Soporte para Escritorio Virtual.
- Política de verificación de la estación de trabajo

8.3.6.14. La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información
8.3.6.15. En la configuración del Escritorio Virtual podrá definirse como mínimo:
- La posibilidad de que el usuario cambie entre escritorio virtual y real.
- La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.
- La posibilidad de utilizar medios removibles desde el escritorio virtual.
- La posibilidad de acceder a recursos compartidos desde el escritorio virtual.
- La posibilidad de imprimir desde el escritorio virtual.
- La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual

8.3.7. Traffic Shapping / QoS
8.3.7.1. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
8.3.7.2. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
8.3.7.3. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

8.3.7.4. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.
8.3.7.5. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo
8.3.7.6. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.
8.3.8. Autenticación y Certificación Digital
8.3.8.1. Capacidad de integrarse con Servidores de Autenticación RADIUS.
8.3.8.2. Capacidad nativa de integrarse con directorios LDAP.
8.3.8.3. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
8.3.8.4. Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
8.3.8.5. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
8.3.8.6. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
8.3.8.7. Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.
8.3.8.8. Soporte de verificación de validación de certificados digitales mediante el protocolo OSCP (Online Simple Enrrollment Protocol).
8.3.8.9. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
8.3.8.10. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
8.3.8.11. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
- Longitud mínima permitida.
- Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
- Expiración de contraseña.

8.3.8.12. Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP
8.3.9. Protección contra intrusos (IPS)
8.3.9.1. El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en SPAN o MIRROR.
8.3.9.2. El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.
8.3.9.3. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.
8.3.9.4. Capacidad de detección de más de 4,000 ataques
8.3.9.5. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
8.3.9.6. El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.
8.3.9.7. El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro

tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.

8.3.9.8. El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).

8.3.9.9. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.

8.3.9.10. Tecnología de detección tipo Stateful basada en Firmas (signatures).

8.3.9.11. Actualización automática de firmas para el detector de intrusos.

8.3.9.12. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.

8.3.9.13. "Mecanismos de detección de ataques:

- Reconocimiento de patrones y Análisis de protocolos.
- Detección de anomalías.
- Detección de ataques de RPC (Remote procedure call).
- Protección contra ataques de Windows o NetBios.
- Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)
- Protección contra ataques DNS (Domain Name System)
- Protección contra ataques a FTP, SSH, Telnet y Rlogin
- Protección contra ataques de ICMP (Internet Control Message Protocol)."

8.3.9.14. "Métodos de notificación:

8.3.9.15. Alarmas mostradas en la consola de administración del "appliance".

- Alertas vía correo electrónico.
- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto."
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

8.3.10. Prevención de Fuga de Información (DLP)

8.3.10.1. La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.

8.3.10.2. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.

8.3.10.3. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.

8.3.10.4. Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.

8.3.10.5. En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.

8.3.10.6. La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.

8.3.10.7. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

8.3.11. Control de Aplicaciones

8.3.11.1. Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.

8.3.11.2. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

8.3.11.3. La solución debe tener un listado de al menos 3,000 aplicaciones ya definidas por el fabricante.

8.3.11.4. El listado de aplicaciones debe actualizarse periódicamente.

8.3.11.5. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.

8.3.11.6. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.

8.3.11.7. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.

8.3.11.8. Preferentemente deben soportar mayor granularidad en las acciones.

8.3.12. Inspección de Contenido SSL

8.3.12.1. La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.

8.3.12.2. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).

8.3.12.3. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

8.3.12.4. Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.

8.3.13. Antivirus

8.3.13.1. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.

8.3.13.2. El Antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.

8.3.13.3. Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.

8.3.13.4. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.

8.3.13.5. La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo "appliance", que permita la aplicación de esta protección por política de control de acceso.

8.3.13.6. El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.

8.3.13.7. El "appliance" deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List).

8.3.13.8. El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos Http, FTP, IMAP, POP3, SMTP.

8.3.13.9. El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.

8.3.13.10. El Antivirus deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.

8.3.13.11. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
8.3.13.12. El antivirus deberá ser capaz de filtrar archivos por extensión.
8.3.13.13. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo.
8.3.13.14. Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
8.3.13.15. Las firmas de antivirus deberán ser del mismo fabricante que el "appliance".
8.3.13.16. El sistema debe ser capaz de integrarse a futuro con una solución de sanboxing del mismo fabricante de manera que se pueda aprovechar las firmas generadas en el Firewall.

8.3.14. AntiSpam
8.3.14.1. La capacidad AntiSpam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
8.3.14.2. La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
8.3.14.3. La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM.
8.3.14.4. En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

8.3.15. Filtrado de URLs (URL Filtering)
8.3.15.1. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
8.3.15.2. Debe poder categorizar contenido Web requerido mediante IPv6.
8.3.15.3. Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
8.3.15.4. Configurable directamente desde la interfaz de administración del dispositivo "appliance". Con capacidad para permitir esta protección por política de control de acceso.
8.3.15.5. Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
8.3.15.6. Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
8.3.15.7. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
8.3.15.8. La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing.
8.3.15.9. La solución deberá de ser capaz de poder bloquear el acceso cuentas de dominios específicos a servicios de Google como por ejemplo GMail, Gdocs.

8.3.15.10. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.

8.3.15.11. Será posible exceptuar la inspección de HTTPS por categoría.

8.3.15.12. Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo.

8.3.16. Alta Disponibilidad

8.3.16.1. Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.

8.3.16.2. Alta Disponibilidad en modo Activo-Pasivo.

8.3.16.3. Alta Disponibilidad en modo Activo-Activo.

8.3.16.4. Posibilidad de definir al menos dos interfaces para sincronía.

8.3.16.5. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.

8.3.16.6. Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.

8.3.17. Características de Administración

8.3.17.1. Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).

8.3.17.2. La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.

8.3.17.3. Interfaz basada en línea de comando (CLI) para administración de la solución.

8.3.17.4. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.

8.3.17.5. Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).

8.3.17.6. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.

8.3.17.7. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.

8.3.17.8. El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.

8.3.17.9. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.

8.3.17.10. Soporte de SNMP versión 2 y Soporte de SNMP versión 3.

8.3.17.11. Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.

8.3.17.12. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.

8.3.17.13. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.

8.3.17.14. Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.

8.3.17.15. Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.

8.3.18. Virtualización

8.3.18.1. El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
8.3.18.2. La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
8.3.18.3. Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.
8.3.18.4. Cada instancia virtual debe poder tener un administrador independiente
8.3.18.5. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
8.3.18.6. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
8.3.18.7. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
8.3.18.8. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
8.3.18.9. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

8.3.19. Licenciamiento, Soporte y Actualizaciones
8.3.19.1. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios y conexiones limitándola solamente por el desempeño del equipo.
8.3.19.2. La vigencia de licencia de actualización debe incluirse la capacidad de poder hacer actualizaciones de firmas IPS, URL Filtering, antispam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo con las características arriba descritas, por espacio mínimo de 1 año.
8.3.19.3. La solución debe contar con un Centro de Investigación propio del mismo fabricante para la actualización de políticas
8.3.19.4. El equipo debe de incluir Soporte Telefónica, Reemplazo de Fábrica, Actualizaciones de Firmware por 1 año.
8.3.19.5. El fabricante deberá contar con un centro de atención al cliente (TAC) basado en la ciudad de México con atención y soporte en lenguaje inglés y Español. Además de un soporte mundial tipo "follow-the-sun".

8.3.20. Capacidades de desempeño
- El equipo debe contar con un Throughput Firewall de al menos 60 Gbps para paquetes de 512 bytes de UDP y 6 Gigabytes para para paquetes de 64 bytes, el desempeño de Firewall aplica tanto para tráfico IPv4 como IPv6.
- El equipo debe contar con un Throughput VPN IPSec de por lo menos 50 Gbps.
- El equipo debe contar con un Throughput VPN SSL de por lo menos 3.5 Gbps.
- El equipo debe contar con un Throughput IPS de al menos 12 Gbps.
- El equipo debe contar con un Throughput de Firewall de Nueva Generación (NGFW) de al menos 10 Gbps.
- El equipo debe contar con un Throughput de inspección de tráfico SSL de por lo menos 7 Gbps.
- El equipo debe contar con al menos 7.5 millones de Sesiones concurrentes.
- El equipo debe soportar al menos 500,000 Nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 5000 usuarios de VPN SSL.
- El equipo debe poder generar al menos 50000 VPN's IPSec Client to Gateway y 5000 VPN's IPSec Gateway to Gateway.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 10 virtual Firewalls.
- De igual forma el desempeño en next generation firewall mode de al menos 10 Gb/s
- Desempeño en firewall de aplicaciones de al menos 28 Gb/s.

- El equipo debe contar con al menos 15 Interfaces GigaEthernet RJ45 aceleradas por hardware y 5 puertos ethernes SPF.
- El equipo debe contar con al menos 4 interfaces 10GigaEthernet PLUS Y 4 interfaces 10GigaEthernet PLUS Ultra low latency.
- El equipo debe contar una fuente de poder redundante para N+1.

8.4. **Plataforma de seguridad para nube pública**

Como parte de la infraestructura de seguridad que deberá habilitarse, el proveedor deberá considerar una plataforma de soluciones de ciberseguridad que deberá ser implementada en la nube pública en la que serán hospedadas las aplicaciones e instancias del cliente. Además, estas soluciones de nube (las cuales serán descritas más adelante) deberán ser del mismo fabricante que las soluciones de Next Generation Firewall, SD-WAN, Switches de datos y puntos de acceso inalámbricos que se instalarán en los distritos y los demás edificios (sitios remotos) de manera física. Con esto, se pretende cumplir con el principio de consolidación de fabricantes que Gartner recomienda. Esto provee como principal beneficio la reducción en la complejidad y el mejoramiento en la postura ante riesgos de manejo, configuración y soporte.

El proveedor deberá, para este proyecto, contar con un esquema que permita crecer de manera paulatina, y conforme se vaya requiriendo las capacidades de las soluciones de seguridad en nube que se propondrán.

El principal objetivo es permitir que, durante los días de mayor demanda, se tenga la capacidad de incrementar los modelos de máquinas virtuales de las herramientas, con las que se podrá soportar mayor demanda en los picos más altos de acceso.

El proveedor adquirirá un modelo de licencias basadas en el consumo, el cual deberá ser suficiente para soportar las demandas de tráfico a inspeccionar durante las etapas de desarrollo, pruebas, simulacros y el día de las elecciones y posteriores.

- La solución debe permitir crear, cambiar, suspender las licencias generadas en cualquier momento, a través de una interfaz web (portal) y API REST.
- Ambas formas de acceso deberán realizarse a través de cuentas y perfiles de acceso, tanto de usuarios como de aplicaciones, de forma independiente.
- El portal de gestión de estos accesos debe tener un perfil administrativo para gestionar accesos exclusivos de administradores.
- Debe permitir automatizar el proceso de creación e instalación de licencias utilizando, como mínimo, Terraform, Ansible Galaxy y python.
- El portal debe permitir el seguimiento del consumo de las siguientes formas:
  - ✓ Consumo histórico.
  - ✓ Ingesta diaria.
  - ✓ Consumo medio de los últimos 30 días.
  - ✓ Valor total de las unidades de consumo disponibles para su uso.
  - ✓ Contar con un mecanismo de alerta, en base al consumo promedio de los últimos 30 días, notificando que los créditos por unidades de consumo se agotarán con 90, 60, 30, 15, 7 días de anticipación.
- El portal debe tener una forma de estimar el número de unidades de consumo de acuerdo con la configuración elegida y el alcance de los servicios de licencia.
- El portal debe permitir definir plantillas de configuración para generar licencias
- Cada plantilla de configuración debe permitir definir al menos:
  - ✓ Capacidad de procesamiento de licencias.
  - ✓ Activar o desactivar servicios adicionales o suscripciones.
- Debe ser posible cambiar los parámetros de una plantilla de configuración a través del portal web o API REST.

- Cualquier cambio en una plantilla de configuración se propagará automáticamente a todas las licencias generadas en función de ella antes y después del cambio.
- Las licencias generadas en el portal podrán ser instaladas en nubes públicas o privadas

A continuación, se describen las distintas herramientas que deberán ser implementadas en la nube pública seleccionada por el cliente, y que serán aprovisionadas a través del licenciamiento del esquema flexible mencionado previamente. Tal como se mencionó, las cuatro soluciones siguientes deberán ser del mismo fabricante que las implementadas en los distritos y ubicaciones físicas.

8.4.1.Next Generation Firewall

Gracias al modelo flexible de licenciamiento, se podrá incrementar la capacidad de la máquina virtual seleccionada con base en los requerimientos de las distintas etapas del proceso electoral, por lo que las especificaciones técnicas podrán variar:

- Standalone o HA (Alta disponibilidad)
- Soporte de 1 vCPU – 16 vCPU
- Máximo almacenamiento de 32 GB - 2TB
- Máximo de políticas de firewall: 10,000 – 200,000
- Máximo número de endpoints registrados: 2,000 – 20,000
- El número de interfaces de red dependerá de la VM seleccionada para montar el firewall en la nube pública (máximo: 24)
- Soporte de nubes públicas:
  - ✓ Amazon AWS
  - ✓ VMware Cloud on AWS
  - ✓ VMware Cloud on Dell EMC
  - ✓ Microsoft Azure
  - ✓ Google GCP (Google Cloud Platform)
  - ✓ Oracle OCI
  - ✓ Alibaba Cloud (AliCloud)
  - ✓ IBM Cloud (Gen1 / Gen2)

8.4.1.1. **El Next Generation Firewall deberá soportar las siguientes funcionalidades:**

General

- Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- Debe ser compatible con NAT64 y NAT46;
- Debe implementar el protocolo ECMP;
- Debe soportar SD-WAN de forma nativa;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- Debe soporta protección contra la suplantación de identidad (anti-spoofing);
- Implementar la optimización del tráfico entre dos dispositivos;
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Soportar OSPF graceful restart;
- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo;

- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
- Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
- El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
- Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
- La consola de administración debe soportar español;
- La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad;
- La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

8.4.1.2. **Firewall**

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes;
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN;
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

8.4.1.3. **APP Control (Control de aplicaciones)**

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;

- Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

8.4.1.4. **Threat Prevention (Prevención de Intrusos)**

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;

- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
- Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).

8.4.1.5. **URL Filter (Filtro URL)**

- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);

- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente.

8.4.1.6. **User Identity (Identidad de Usuario)**

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control, basados en usuarios y grupos de usuarios;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control, basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control, basados en usuarios y grupos de usuarios;
- Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control, basados en usuarios y grupos de usuarios;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores.

8.4.1.7. **QoS & Shaping (Control de tráfico)**

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;

- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

8.4.1.8. **DLP (Prevención de perdida de datos)**

- Permite la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.

8.4.1.9. **Geo IP**

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

8.4.1.10. **VPN**

- Soporte de VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
- Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
- Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Cada firewall deberá incluir el licenciamiento necesario para activar los siguientes elementos de seguridad y recibir actualizaciones de los mismos durante el periodo contratado:

- Antivirus
- Mobile Malware
- Cloud Sandbox
- IPS
- Application Control
- Filtrado URL, DNS y Vídeo
- Servicio de Antispam

Asimismo, cada solución implementada deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo
- Portal de administración de los activos

8.4.2. WEB APPLICATION FIREWAL (WAF)

Gracias al modelo flexible de licenciamiento, se podrá incrementar la capacidad de la máquina virtual seleccionada con base en los requerimientos de las distintas etapas del proceso electoral, por lo que las especificaciones técnicas podrán variar:

- ✓ Standalone o HA (Alta disponibilidad)
- ✓ Soporte de 1 vCPU – 8 vCPU
- ✓ Throughput soportado: 25 Mbps – 3 Gbps
- ✓ Aplicaciones soportadas: ilimitado
- ✓ Número de interfaces de red soportadas: 1 – 10
- ✓ Máximo almacenamiento de 40 GB - 2TB
- ✓ Memoria recomendada: 8 GB – 32 GB

8.4.2.1. Características Generales

- La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso, Transparente en Línea y Sniffer.
- La solución debe de ser capaz de ser implementada con protocolo WCCP.
- Soportar VLANs del estándar IEEE 802.1q.
- Soportar direccionamiento IPv4 y IPv6 en las interfaces de red y virtuales (VLANs).

- La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo de la instancia principal.
- La solución debe de soportar enrutamiento por política (policy route)
- El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente al equipo por puerto de consola, o remotamente vía SSH.
- Debe de soportar administración basada en interfaz web HTTP.
- Debe de soportar administración basada en interfaz de línea de comando vía Telnet.
- Tener la función de auto-completar comandos en la CLI.
- Tener ayuda contextual en la CLI.
- La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de serie, modo de operación, tiempo en servicio, versión de firmware)
- Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte.
- La solución ofertada deberá de tener acceso a la línea de comando CLI directamente a través de la interfaz gráfica de gestión (GUI).
- Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión.
- Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria
- Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados.
- Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema.
- Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema.
- Tener un dashboard de visualización con información de las interfaces de red del sistema.
- La configuración de administración de la solución debe permitir la utilización de perfiles.
- Debe de ser posible ejecutar y recuperar el respaldo por la interfaz Web (GUI).
- Debe de tener la opción de cifrar el respaldo utilizando algoritmo AES 128-bit o superior.
- Debe de ser posible ejecutar y recuperar el respaldo utilizando FTP.
- Debe de ser posible ejecutar y recuperar el respaldo utilizando SFTP y TFTP.
- Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3.
- Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog.
- La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG.
- Debe tener la capacidad de almacenar los logs en un appliance remoto.
- La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías.
- La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web.
- La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen
- Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario.
- Debe soportar RESTFULL API para gestión de la configuración.

8.4.2.2. Características de autenticación

- Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP/HTTPS.
- Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos
- La solución debe de ser capaz de autenticar los usuarios a través de certificados digitales personales.
- Debe tener base local para almacenamiento y autenticación de los usuarios.
- La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP, RADIUS y SAML.
- La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM.
- La solución debe de ser capaz de crear grupos de usuarios para configurar mecanismos de autenticación por grupos.
- Debe soportar CAPTCHA y Real Browser Enforcement (RBE).
- Debe soportar autenticación de doble factor.

8.4.2.3. Características regulatorias y de cumplimiento.

- La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP
- El equipo debe de tener certificación FCC Class A part 15
- El equipo debe de tener certificación C-Tick
- El equipo debe de tener certificación VCCI
- El equipo debe de tener certificación CE
- El equipo debe de tener certificación UL/cUL
- El equipo debe de tener certificación CB.

8.4.2.4. Características de Web Application Firewall

- Debe tener soporte nativo de HTTP/2.
- Debe soportar traducción de HTTP/2 a HTTP 1.1.
- Deberá soportar interoperabilidad con OpenAPI 3.0.
- Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica.
- La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus.
- Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no.
- Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial.
- Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo.
- El perfil aprendido de forma automática debe de poder ser ajustado.
- Tener la capacidad de creación de firmas de ataques personalizables.
- Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol.
- Tener la capacidad de protección contra ataques del tipo Botnet.
- Tener la capacidad de protección contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST).

- La solución debe tener funcionalidad de protección contra ataques como acceso por fuerza bruta.
- Debe soportar detección de ataques de Clickjacking.
- Debe soportar detección de ataques de cambios de cookie.
- Identificar y proteger contra ataques del tipo Credit Card Theft.
- Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF).
- La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS).
- Debe tener protección contra ataques de Denial of Service (DoS);
- Tener la capacidad de protección contra ataques del tipo HTTP header overflow.
- Tener la capacidad de protección contra ataques del tipo Local File inclusion (FLI).
- Tener la capacidad de protección contra ataques del tipo Man-in-the0middle (MITM).
- Tener la capacidad de protección contra ataques del tipo Remote File Inclusion (RFI).
- Tener la capacidad de protección contra ataques del tipo Server Information Leakage.
- Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);
- Tener la capacidad de protección contra ataques del tipo Malformed XML.
- Identificar y prevenir ataques del tipo Low-rate DoS.
- Prevención contra Slow POST attack.
- Proteger contra ataques Slowloris.
- Tener la capacidad de protección contra ataques del tipo SYN flood.
- Tener la capacidad de protección contra ataques del tipo Forms Tampering.
- La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos.
- Tener la capacidad de protección contra ataques del tipo Directory Traversal.
- Tener la capacidad de protección del tipo Access Rate Control.
- Identificar y proteger contra Zero Day Attacks.
- Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold.
- Permitir configurar reglas de bloqueo a métodos HTTP no deseados.
- Permitir que se configuren reglas de límite de upload por tamaño del archivo.
- Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país.
- Debe soportar crear políticas de geolocalización, permitiendo que el tráfico de determinado país sea bloqueado.
- Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen.
- Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución.
- Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
- Tener la capacidad de conectarse a una base de datos en Internet para validar que las credenciales que usan los usuarios para acceder a algún sistema no sean credenciales robadas.
- Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdida de información del encabezado HTTP.
- Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo.
- Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo.
- Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado.

- La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico.
- Para SSL/TLS offload soportar al menos SSL 3.0, TLS 1.0, 1.1 e 1.2.
- La solución debe tener la capacidad de almacenar certificados digitales de CA's.
- La solución debe de ser capaz de generar CSR para ser firmado por una CA.
- La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL.
- La solución debe contener las firmas de robos conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones.
- La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación deberá ser actualizada automáticamente.
- La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores.
- La solución debe permitir la customización o reenvío de solicitaciones y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location.
- La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- La solución debe de tener la capacidad de definir restricciones a determinados métodos HTTP
- La solución debe tener la capacidad de proteger contra detección de campos ocultos.
- Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares.
- La solución debe permitir la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, etc, para proveer parches virtuales.
- Debe generar un perfil de protección automáticamente a partir de reporte en formato XML generado por un scanner de vulnerabilidad de terceros.
- Debe permitir programar la verificación de vulnerabilidades.
- La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML.
- Soportar redirección y reescritura de requisiciones y respuestas HTTP.
- Permitir redirección de requisiciones HTTP para HTTPS.
- Permitir reescribir la línea URL del encabezado de una requisición HTTP.
- Permitir reescribir el campo HOST del encabezado de una requisición HTTP.
- Permitir reescribir el campo REFERER del encabezado de una requisición HTTP.
- Permitir redirigir requisiciones para otro website.
- Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP.
- Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web.
- Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web.
- Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso.
- La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).
- La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación.
- Tener capacidad de caching para aceleración web.
- La solución debe de ser capaz de enviar archivos para solución de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo.
- Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas preexistentes.

8.4.2.5. Características de balanceo de carga

- La solución debe incluir la funcionalidad de balanceo de carga entre servidores web.
- Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS.
- Soportar balanceo / distribución de tráfico y enrutar el contenido hacia distintos servidores web.
- La solución debe permitir crear grupos de servidores (Server Farm / Pool) para distribuir las conexiones de los usuarios.
- Soportar el algoritmo Round Robin para balanceo de carga entre servidores.
- Soportar el algoritmo Weighted Round Robin para balanceo de carga entre servidores.
- Soportar el algoritmo Least Connection para balanceo de carga entre servidores.
- La solución debe de soportar creación de servidores virtuales que definan la interfaz de red/bridge y dirección IP por donde el tráfico con destino al Server Pool es recibido.
- Los servidores virtuales deben de entregar el tráfico hacia un único servidor web y también incluir la opción de distribuir las sesiones/conexiones entre los servidores web del Server Pool.
- Debe de ser posible definir el número máximo de conexiones TCP simultáneas hacia un determinado servidor miembro del Server Pool.
- Permitir prueba de disponibilidad del servidor web a través del método TCP.
- Permitir prueba de disponibilidad del servidor web a través del método ICMP ECHO_REQUEST (ping).
- Permitir prueba de disponibilidad del servidor web a través del método TCP Half Open.
- Permitir prueba de disponibilidad del servidor web a través del método TCP SSL.
- Permitir prueba de disponibilidad del servidor web a través del método HTTP.
- Permitir prueba de disponibilidad del servidor web a través del método HTTPS.
- En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada.
- En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir entre los métodos HEAD, GET y POST.
- En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir el nombre del campo HTTP "host" a ser probado.
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parámetro HTTP".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Direción IP de Origen".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabezado".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie".
- Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509".
- Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y requisiciones HTTP sean contestadas directamente por la solución.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por dirección IP de origen.

- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de cualquier parámetro del header HTTP.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de la URL accedida.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por cookie – método cookie insert y cookie rewrite.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por embedded cookie (cookie original seguido de porción aleatoria).
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Reescritura del Cookie.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Cookie Persistente.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en ASP Session ID.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en PHP Session ID.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en JSP Session ID.
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por sesión SSL.

8.4.2.6. Cada Web Application Firewall deberá incluir el licenciamiento necesario para activar los siguientes elementos de seguridad y recibir actualizaciones de los mismos durante el periodo contratado:

- ✓ Web Security.
- ✓ Reputación IP.
- ✓ Antimalware.
- ✓ Servicio de sandbox en la nube.
- ✓ Defensa contra credential stuffing.
- ✓ Análisis de Amenazas.

Asimismo, cada solución implementada deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- ✓ Soporte a través de un portal Web.
- ✓ Soporte telefónico en español.
- ✓ Actualizaciones del firmware del equipo.
- ✓ Portal de administración de los activos.

8.4.3. Solución centralizada de logging, analíticos y reportes

Se deberá ofertar el suministro, configuración e implementación de una solución, implementada en la nube pública seleccionada por el cliente, que permita proporcionar al usuario una plataforma de administración de logs, analíticos y reportes, la cual debe ser de la misma marca de la solución de dispositivos firewalls, web application firewall. Deberá soportar las siguientes capacidades:

- ✓ Soporte para recolectar logs de todos los dispositivos firewall implementados, tanto en nube como en premisas físicas.
- ✓ Máximo de 500 GB de logs por día
- ✓ Requiere de una VM de mínimo 4 vCPUs
- ✓ Soporte de máximo 12 interfaces de red

- ✓ Mínimo de memoria soportada de 16 GB
- ✓ Aprovisionamiento a través del modelo de licenciamiento flexible

8.4.3.1. Funcionalidades

- Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
- Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3
- Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- Debe permitir activar y desactivar para cada interfaz de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
- Autenticación de usuarios de acceso a la plataforma vía LDAP
- Autenticación de usuarios de acceso a la plataforma vía Radius
- Autenticación de usuarios de acceso a la plataforma vía TACACS+
- Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
- Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
- Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
- Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
- Contar con mecanismos de borrado automático de logs antiguos.
- Permitir la importación y exportación de reportes
- Debe contar con la capacidad de crear informes en formato HTML
- Debe contar con la capacidad de crear informes en formato PDF
- Debe contar con la capacidad de crear informes en formato XML
- Debe contar con la capacidad de crear informes en formato CSV
- Debe permitir exportar los logs en formato CSV
- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
- Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
- La solución debe contar con reportes predefinidos
- Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
- Debe ser posible la duplicación de reportes existentes para su posterior edición.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
- Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
- Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.

- Tener la capacidad de generar y enviar reportes periódicos automáticamente.
- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- Permitir el envío por email de manera automática de reportes.
- Debe permitir que el reporte a enviar por email sea al destinatario específico.
- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
- Debe permitir el uso de filtros en los reportes.
- Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- Permitir especificar el idioma de los reportes creados
- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
- Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
- Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
- Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
- Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
- Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
- Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
- Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
- Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
- Debe permitir visualizar en tiempo real los logs recibidos.
- Debe permitir el reenvío de logs en formato syslog.
- Debe permitir el reenvío de logs en formato CEF (Common Event Format).
- Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red.
- Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red.
- Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
- Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
- Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
- Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
- Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).

- Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC.
- Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3.
- Debe permitir generar alertas de eventos a partir de logs recibidos.
- Debe permitir crear incidentes a partir de alertas de eventos para endpoint.
- Debe permitir la integración al sistema de tickets ServiceNow.
- Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
- Debe permitir respaldar logs en nube.
- Debe soportar el estándar SAML para autenticación de usuarios administradores.

8.4.3.2. Reportes de Next Generation Firewall.

- Debe contar con reporte de cumplimiento de PCI DSS.
- Debe contar con reporte de utilización de aplicaciones SaaS.
- Debe contar con reporte de prevención de perdida de datos (DLP).
- Debe contar con reporte de VPN.
- Debe contar con reporte de Sistema de prevención de intrusos (IPS).
- Debe contar con reporte de reputación de cliente.
- Debe contar con reporte de análisis de seguridad de usuario.
- Debe contar con reporte de análisis de amenaza cibernética.
- Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad.
- Debe contar con reporte de tráfico DNS.
- Debe contar con reporte tráfico de correo electrónico.
- Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red.
- Debe contar con reporte de Top 10 de Websites utilizadas en la red.
- Debe contar con reporte de uso de redes sociales.

8.4.3.3. Wireless Reports.

- Debe contar con reporte de cumplimiento PCI de Wireless.
- Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi.

8.4.3.4. Reportes del Web Application Firewall.

Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web.

8.4.3.5. Se deberá ofertar el licenciamiento necesario para activar los siguientes elementos de seguridad y recibir actualizaciones de los mismos, durante el periodo contratado:

- Servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.

La solución deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo

- Portal de administración de los activos
- Tiempo de respuesta a evento crítico: 1 hora
- Tiempo de respuesta a evento no crítico: Siguiente día hábil.

8.4.4. Herramienta de administración centralizada

El Licitante ganador deberá contar con una herramienta integral de administración centralizada de los dispositivos de seguridad y acceso seguro (NGFW, WAF, Switches y APs) virtuales y físicos, la cual permitirá que, desde una sola consola, tener la administración y visibilidad completa de los dispositivos de red a través de un aprovisionamiento coordinado y herramientas de automatización.

Deberá ser desarrollado por el mismo fabricante que los dispositivos físicos y virtuales de seguridad y red implementados en el proyecto, de tal forma que permita la administración, configuración y monitoreo de la totalidad de dichos dispositivos/instancias. Debe ser tener la capacidad de ser aprovisionado a través del modelo de licenciamiento flexible.

8.4.4.1. **Características y funcionalidades**

- Debe tener la capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.
- Como parte de la visibilidad SD-WAN de los dispositivos gestionados centralmente, la solución debe contar con visibilidad de estado de enlace, desempeño de aplicación, utilización de ancho de banda y cumplimiento de SLA objetivo.
- Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola
- La solución debe tener la capacidad Multi-tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue zerotouch para un aprovisionamiento masivo rápido.
- La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos, conteniendo updates de todos los dispositivos gestionados.
- Debe tener la capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.
- La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
- Permitir integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .
- En la fecha de la propuesta, ninguno de los modelos de la oferta puede estar en el sitio del fabricante en listados de end-of-life o end-of-sales;
- La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS) y API abierta;
- Debe permitir accesos concurrentes de administradores;
- Debe tener interfaz basada en línea de comando para administración de la solución de gestión;
- Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
- Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores;
- Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones;
- Generar alertas automáticas por Email
- Generar alertas automáticas por SNMP
- Generar alertas automáticas por Syslog

- Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario;
- Debe ser permitido al administrador transferir los backups a un servidor FTP.
- Debe ser permitido al administrador transferir los backups a un servidor SCP
- Debe ser permitido al administrador transferir los backups a un servidor SFTP
- Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS+
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI)
- Debe soportar sincronización de reloj interno por protocolo NTP.
- Debe registrar las acciones efectuadas por cualquier usuario.
- Deben proveerse manuales de instalación, configuración y operación de toda la solución, en los idiomas español, o inglés, con presentación de buena calidad.
- Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión.
- Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API).
- Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
- La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización.

8.4.4.2. Administración de los NGFW.

- La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación.
- La gestión debe permitir la creación y administración de políticas de IPS, Antivirus y Anti-Spyware.
- La gestión debe permitir la creación y administración de políticas de Filtro de URL.
- Permitir buscar cuáles reglas un objeto está siendo utilizado.
- Permitir la creación de reglas que permanezcan activas en horario definido.
- La solución debe permitir ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados.
- Debe tener capacidad de desplegar los resultados de auditoría de seguridad de los dispositivos gestionados.
- Permitir backup de las configuraciones y rollback de configuración para la última configuración salva.
- Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing).
- Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas.
- Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión.

- La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta.
- La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos.
- Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados.
- Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador.
- Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos.
- Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
- Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware.
- Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos.
- Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración.
- Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos.
- Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión.
- Permitir configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada.
- Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos.
- Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada.
- Permitir la creación de reglas anti DoS de forma centralizada.
- Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada.
- Debe permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía.
- Debe permitir el uso de DDNS en VPNs de manera centralizada.
- Debe permitir la gestión de Access Points propietarios de manera centralizada.
- Debe permitir la gestión de Switches propietarios de manera centralizada.
- Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada.

8.4.4.3. La solución deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo
- Portal de administración de los activos
- Tiempo de respuesta a evento crítico: 1 hora
- Tiempo de respuesta a evento no crítico: Siguiente día hábil.

8.5. **Switches de datos**

Se deberán integrar 26 switches de datos de 24 puertos (21 para Juntas Electorales Distritales, 1 para CCV, 1 para Almacén General, 1 para Edificio Sede, 1 para Edificio de Hidalgo,1 para Oficinas Centrales), de la misma marca y modelo que los equipos UTM y de las soluciones virtuales montadas en la infraestructura de nube. Estos equipos deben contar al menos con las siguientes especificaciones:

- 12 Puertos 1 GE RJ45
- 12 Puertos 1 GE RJ45 Power Over Ethernet (POE)
- 4 Puertos GE SFP
- Budget PoE: 185 W
- 1 puerto consola serial RJ-45
- Factor de Forma: 1 RU
- Capacidad de Switching: 56 Gbps
- Paquetes Por Segundo: 83 Mpps
- Almacenamiento de direcciones MAC: 8K
- Latencia de Red: < 4µs
- Tamaño de "Link Aggregation Group": 8
- Total de Grupos de Link Aggregation: 8
- Buffers de Paquetes: 512 KB
- Instancias de Spanning Tree: 16
- DRAM: 256 MB
- FLASH: 32 MB

Características de Administración:

- El switch deberá poder aceptar actualizaciones de firmware
- Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE
- Deberá soportar detección y notificación de conflictos de direcciones IP
- Deberá soportar administración en la nube
- Deberá soportar administración por IPv4 e IPv6
- Deberá soportar Telnet / SSH para acceso a la consola
- Deberá soportar HTTP / HTTPS
- Deberá soportar SNMP v1/v2c/v3
- Deberá poder configurar su reloj mediante un NTP Server
- Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
- Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
- Deberá soportar HTTP REST APIs para configuración y monitoreo

Alta Disponibilidad:

- Deberá soportar Multi-Chassis LAG (MCLAG)
- Deberá soportar STP sobre Multi-Chassis LAG (MCLAG)

Calidad de servicio

- Deberá soportar priorización de tráfico basada en 802.1p
- Deberá soportar priorización de tráfico basada en IP TOS/DSCP
- Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP

Capa 2

- Deberá soportar Link Aggregation estático

- Deberá soportar LACP
- Deberá soportar Spanning Tree
- Deberá soportar Jumbo Frames
- Deberá soportar Auto negociación para la velocidad de los puertos y para dúplex
- Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
- Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Deberá soportar la funcionalidad STP Root Guard
- Deberá soportar STP BPDU Guard
- Deberá soportar Edge Port / Port Fast
- Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
- Deberá soportar Private VLAN
- Deberá soportar el estándar IEEE 802.3ad Link Aggregation con LACP
- Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- Deberá soportar el estándar IEEE 802.1AX Link Aggregation
- Deberá soportar instancias de Spanning Tree (MSTP/CST)
- Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
- Deberá soportar el estándar IEEE 802.3 10Base-T
- Deberá soportar el estándar IEEE 802.3u 100Base-TX
- Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX
- Deberá soportar el estándar IEEE 802.3ab 1000Base-T
- Deberá soportar el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física
- Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
- Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
- Deberá soportar la funcionalidad de Virtual-Wire
- Deberá soportar Time-Domain Reflectometer (TDR)
- Deberá soportar 4094 VLANs simultáneas
- Deberá soportar IGMP Snooping
- Deberá soportar IGMP proxy y querier
- Deberá soportar emergency location identifier numbers (ELINs) en LLDP-MED
- Deberá permitir la negociación de POE en LLDP-MED
- Deberá permitir limitar la cantidad de MACs aprendidas por puerto
- Deberá permitir un mínimo de 15 instancias de MSTP
- Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
- Deberá soportar un mecanismo de detección y prevención de loops
- Deberá soportar VLAN Stacking (QinQ)
- Deberá soportar SPAN
- Deberá soportar RSPAN y ERSPAN

RFCs

- Deberá soportar el RFC 2571 Architecture for Describing SNMP
- Deberá soportar DHCP Client
- Deberá soportar el RFC 854 Telnet Server
- Deberá soportar el RFC 2865 RADIUS
- Deberá soportar el RFC 1643 Ethernet-like Interface MIB
- Deberá soportar el RFC 1213 MIB-II

- Deberá soportar el RFC 1354 IP Forwarding Table MIB
- Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching
- Deberá soportar el RFC 1573 SNMP MIB II
- Deberá soportar el RFC 1157 SNMPv1/v2c
- Deberá soportar el RFC 2030 SNTP

Seguridad & Visibilidad

- Deberá soportar Port Mirroring
- Deberá soportar Admin Authentication Via RFC 2865 RADIUS
- Deberá soportar el estándar IEEE 802.1x authentication Port-based
- Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
- Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
- Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
- Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
- Deberá soportar Radius CoA (Change of Authority)
- Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- Deberá soportar el estándar IEEE 802.1ab LLDP-MED
- Deberá soportar Radius Accounting
- Deberá soportar EAP pass-through
- Deberá soportar detección de dispositivos
- Deberá soportar MAC-IP binding
- Deberá soportar sFlow
- Deberá soportar Flow Export
- Deberá soportar ACLs
- Deberá soportar múltiples ACLs de ingreso
- Deberá soportar scheduling de ACLs
- Deberá soportar DHCP Snooping
- Deberá soportar listas de servidores DHCP permitidos
- Deberá soportar bloqueo de DHCP
- Deberá permitir Dynamic ARP Inspection (DAI)
- Deberá permitir Access VLANs
- Deberá permitir tagging de tráfico con VLAN ID mediante ACLs

Otras funcionalidades

- Deberá soportar Syslog
- Debe contar con un sensor de temperatura interno
- Debe permitir monitorear la temperatura del dispositivo
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)

Soporte y garantía

Cada equipo deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Reemplazo en caso de fallo
- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo

- Portal de administración de los activos
- Tiempo de respuesta a evento crítico: 1 hora
- Tiempo de respuesta a evento no crítico: Siguiente día hábil.

Se deberán integrar 1 switch de datos de 48 puertos para el CCV (Centro de Captura y Verificación) de la misma marca y modelo que los equipos UTM y de las soluciones virtuales montadas en la infraestructura de nube. Estos equipos deben contar al menos con las siguientes especificaciones:

- 24 Puertos 1 GE RJ45
- 24 Puertos 1 GE RJ45 Power Over Ethernet (POE)
- 4 Puertos GE SFP
- Budget PoE: 370 W
- 1 puerto consola serial RJ-45
- Factor de Forma: 1 RU
- Capacidad de Switching: 105 Gbps
- Paquetes Por Segundo: 155 Mpps
- Almacenamiento de direcciones MAC: 16K
- Latencia de Red: 4µs
- Tamaño de "Link Aggregation Group": 8
- Total de Grupos de Link Aggregation: 16
- Buffers de Paquetes: 1.5 MB
- DRAM: 256 MB
- FLASH: 64 MB
- Temp [°C]: 0-45

Característica de Administración

- El switch deberá poder aceptar actualizaciones de firmware
- Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE
- Deberá soportar detección y notificación de conflictos de direcciones IP
- Deberá soportar administración en la nube
- Deberá soportar administración por IPv4 e IPv6
- Deberá soportar Telnet / SSH para acceso a la consola
- Deberá soportar HTTP / HTTPS
- Deberá soportar SNMP v1/v2c/v3
- Deberá poder configurar su reloj mediante un NTP Server
- Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
- Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
- Deberá soportar HTTP REST APIs para configuración y monitoreo

Alta Disponibilidad

- Deberá soportar Multi-Chassis LAG (MCLAG)
- Deberá soportar STP sobre Multi-Chassis LAG (MCLAG)

Calidad de servicio

- Deberá soportar priorización de tráfico basada en 802.1p
- Deberá soportar priorización de tráfico basada en IP TOS/DSCP
- Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP

Capa 2

- Deberá soportar Link Aggregation estático
- Deberá soportar LACP
- Deberá soportar Spanning Tree
- Deberá soportar Jumbo Frames
- Deberá soportar Auto negociación para la velocidad de los puertos y para dúplex
- Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
- Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Deberá soportar la funcionalidad STP Root Guard
- Deberá soportar STP BPDU Guard
- Deberá soportar Edge Port / Port Fast
- Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
- Deberá soportar Private VLAN
- Deberá soportar el estándar IEEE 802.3ad Link Aggregation con LACP
- Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- Deberá soportar el estándar IEEE 802.1AX Link Aggregation
- Deberá soportar instancias de Spanning Tree (MSTP/CST)
- Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
- Deberá soportar el estándar IEEE 802.3 10Base-T
- Deberá soportar el estándar IEEE 802.3u 100Base-TX
- Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX
- Deberá soportar el estándar IEEE 802.3ab 1000Base-T
- Deberá soportar el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física
- Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
- Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
- Deberá soportar la funcionalidad de Virtual-Wire
- Deberá soportar Time-Domain Reflectometer (TDR)
- Deberá soportar 4094 VLANs simultáneas
- Deberá soportar IGMP Snooping
- Deberá soportar IGMP proxy y querier
- Deberá soportar emergency location identifier numbers (ELINs) en LLDP-MED
- Deberá permitir la negociación de POE en LLDP-MED
- Deberá permitir limitar la cantidad de MACs aprendidas por puerto
- Deberá permitir un mínimo de 15 instancias de MSTP
- Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
- Deberá soportar un mecanismo de detección y prevención de loops
- Deberá soportar VLAN Stacking (QinQ)
- Deberá soportar SPAN
- Deberá soportar RSPAN y ERSPAN

RFCs

- Deberá soportar el RFC 2571 Architecture for Describing SNMP
- Deberá soportar DHCP Client
- Deberá soportar el RFC 854 Telnet Server

- Deberá soportar el RFC 2865 RADIUS
- Deberá soportar el RFC 1643 Ethernet-like Interface MIB
- Deberá soportar el RFC 1213 MIB-II
- Deberá soportar el RFC 1354 IP Forwarding Table MIB
- Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching
- Deberá soportar el RFC 1573 SNMP MIB II
- Deberá soportar el RFC 1157 SNMPv1/v2c
- Deberá soportar el RFC 2030 SNTP

Seguridad & Visibilidad

- Deberá soportar Port Mirroring
- Deberá soportar Admin Authentication Via RFC 2865 RADIUS
- Deberá soportar el estándar IEEE 802.1x authentication Port-based
- Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
- Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
- Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
- Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
- Deberá soportar Radius CoA (Change of Authority)
- Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- Deberá soportar el estándar IEEE 802.1ab LLDP-MED
- Deberá soportar Radius Accounting
- Deberá soportar EAP pass-through
- Deberá soportar detección de dispositivos
- Deberá soportar MAC-IP binding
- Deberá soportar sFlow
- Deberá soportar Flow Export
- Deberá soportar ACLs
- Deberá soportar múltiples ACLs de ingreso
- Deberá soportar scheduling de ACLs
- Deberá soportar DHCP Snooping
- Deberá soportar listas de servidores DHCP permitidos
- Deberá soportar bloqueo de DHCP
- Deberá permitir Dynamic ARP Inspection (DAI)
- Deberá permitir Access VLANs
- Deberá permitir tagging de tráfico con VLAN ID mediante ACLs

Otras funcionalidades

- Deberá soportar Syslog
- Debe contar con un sensor de temperatura interno
- Debe permitir monitorear la temperatura del dispositivo
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)

Soporte y garantía

Cada equipo deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Reemplazo en caso de fallo
- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo
- Portal de administración de los activos
- Tiempo de respuesta a evento crítico: 1 hora
- Tiempo de respuesta a evento no crítico: Siguiente día hábil.

8.6. **Puntos de acceso inalámbricos**

Se deberán integrar 52 puntos de acceso inalámbricos (42 para Juntas Electorales Distritales, 4 para Oficinas Centrales, 2 para CCV, 2 para Almacén General, 2 para Edificio Sede), de la misma marca y modelo que los equipos UTM y de las soluciones virtuales montadas en la infraestructura de nube. Estos equipos deben contar al menos con las siguientes especificaciones:

- Tipo: para interiores (Indoor)
- Throughput: 867 Mbps
- Clientes concurrentes recomendados por radio: 30
- Número máximo de clientes concurrentes por radio: 512
- Tecnologías: 802.11 a/b/g/n/ac
- Frecuencias de operación: 2.4 / 5 GHz
- Cantidad de radios: 2
- SU-MIMO: 2x2
- 802.11ac Wave2: 1
- MU-MIMO: 1
- 802.11ac VHT [MHz]: 20/40/80
- Potencia máxima de transmisión: 24 dBm
- Sensibilidad RX mínima: -91 dBm
- Flujo espacial: 2
- Antenas Externas: 0
- Antenas Internas: 4
- Ganancia Antenas Externa [dBi @ 2.4Ghz]: 0
- Ganancia Antenas Externa [dBi @ 5Ghz]: 0
- Ganancia Antenas Internas [dBi @ 2.4Ghz]: 4
- Ganancia Antenas Internas [dBi @ 5Ghz]: 5
- Antenas Internas BLE: 1
- Antena BLE [dBi]: 0
- Interfaces ethernet: 1 GE
- IEEE 802.3az: 1
- 12VDC: 1
- Kensington Lock: 1
- Temperatura máxima de operación: 45 ° C
- Analizador de espectro: 1
- Mesh: 1

Características Generales

- Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la wireless y que pueda ser configurado de manera centralizado a través de un controlador inalámbrico;

- Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;
- Debe identificar automáticamente el controlador inalámbrico al que se conectará;
- Debe permitir administrarse remotamente a través de links WAN;
- Debe poseer capacidad dual-band con radios 2.4GHz y 5GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;
- El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico;
- Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;
- Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;
- Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;
- En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;
- Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;
- Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;
- En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);
- En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;
- En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
- En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;
- Debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
- Debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
- Debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming;
- Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
- Debe implementar el estándar IEEE 802.11e;
- Debe implementar el estándar IEEE 802.11h;
- El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU;
- El punto de acceso deberá soportar (LPDC) - Low Density Parity Check;
- El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;
- El Punto de Acceso deberá soportar metodo de diversidad (MRC) Maximum Ratio Combining;
- Debe tener indicadores luminosos (LED) para indicación de estado;

- Debe permitir su alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3af o 802.3at;
- El punto de acceso debe ser compatible y ser administrado por los controladores inalámbricos de este proceso;
- Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
- Debe poseer un certificado emitido por la Wi-Fi Alliance;

Cada equipo deberá incluir el servicio de soporte 24x7x365 que considere lo siguiente:

- Reemplazo en caso de fallo
- Soporte a través de un portal Web
- Soporte telefónico en español
- Actualizaciones del firmware del equipo
- Portal de administración de los activos
- Tiempo de respuesta a evento crítico: 1 hora
- Tiempo de respuesta a evento no crítico: Siguiente día hábil.

8.7. Requerimiento del Licitante para los componentes de ciberseguridad

Dado lo crítico que es el tema de la ciberseguridad en el proceso electoral se requiere que:

- El Licitante deberá presentar en su oferta, cartas por parte del fabricante de la solución de ciberseguridad, donde especifique que su representante tiene al menos nivel de certificación avanzado y que a la fecha del concurso, cuenta con la autorización para comercializar las soluciones requeridas a precios preferenciales y cuenta como experiencia en proyectos de seguridad similares.
- El Licitante deberá contar con al menos con 2 ingenieros certificados, y al menos un arquitecto de seguridad en redes y firewalls empresariales y además cuente con certificación de seguridad para la nube propuesta por parte del fabricante, tanto en analíticos como administración centralizada. Esto para mantener una homogeneidad en las soluciones administradas de todos los distritos
- El Licitante deberá presentar en su oferta, cartas de referencia de proyectos similares de preferencia gubernamentales y al menos una del sector privado, debidamente firmadas y selladas por parte del usuario final, donde mencione tiempo de ejecución del proyecto y grado de satisfacción de los servicios del integrador, así también como datos del contacto para verificación del mismo.
- El Licitante ganador deberá otorgar transferencia de conocimiento en sitio, de la solución de ciberseguridad, así como administración de la solución en las instalaciones que el Instituto señale conveniente.

Se requieren tiempos de respuestas menor a 4 horas en caso de contingencia o disrupción de seguridad para que sea atendida cualquier solicitud de manera telefónica, correo electrónico o para cualquier soporte remoto o presencial en caso de así solicitarlo la Secretaría.

De lo anterior se requiere que el Licitante este establecido en la entidad con tiempo anterior al menos a 3 años, esto para confirmar seriedad y tiempos de establecimiento y trayectoria en el campo de la seguridad de la información en el Estado.

Se deberá entregar currículum de los ingenieros con copias originales de las certificaciones en ciberseguridad, esto para evitar cualquier falsificación de documentación la cual será validada con el fabricante.

El Licitante deberá integrar en su propuesta, una carta de compromiso de soporte donde deberá indicar los accesos a algún tipo de herramienta de software en la nube o en sitio web, para levantar tickets de soporte de casos de ciberseguridad y darles seguimiento. Esta herramienta deberá estar disponible durante todo el tiempo de duración del contrato. Así como los números de atención telefónica tanto de oficina como de los ingenieros que estarán soportando la solución.

9. Cláusula de Confidencialidad.

El proveedor del Servicio deberá presentar una carta en papel membretado, debidamente firmada por su representante legal en la que indique que su representada, así como todos los integrantes de su equipo de trabajo que participen del proyecto, se comprometen a mantener la confidencialidad de la información conocida, vista, trabajada o producida durante el desarrollo del proyecto.

Adicionalmente, el proveedor del Servicio deberá apegarse en todo momento a Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

"ANEXO 5"

31904.- Servicios Integrales de Infraestructura de Cómputo
REQUISICIÓN DA/CRM/151/2024
LOTE 2

Lote	Descripción	Cantidad Total	Sitios requeridos	Periodo de uso
2	Servicio de arrendamiento de cámaras IP tipo bala, que incluye el **suministro, instalación, configuración y desmantelamiento**, para solución de **CCTV** para las Juntas Electorales Distritales, Edificio de Méndez Centro de Captura y Verificación (CCV), Edificio de Periférico Centro de Acopio y Transmisión de Datos (CATD) para el IEPC Tabasco.	49 Cámaras	42 son para las 21 Juntas Electorales Distritales, 2 para Edificio de Periférico CATD y 5 Edificio de Méndez (CCV)	25 abril al 30 de junio de 2024
	Suministro, instalación, configuración y desmantelamiento, de gabinetes de rack de 19" con 6 unidades de rack	23 Gabinetes	21 Juntas Electorales Distritales, 1 Edificio de Méndez (CCV), 1 Edificio de Periférico (CATD caso fortuito)	25 abril al 30 de junio de 2024
	Suministro, instalación, configuración y desmantelamiento de UPS de 1 unidad de rack	23 UPS	21 Juntas Electorales Distritales, 1 Edificio de Méndez (CCV), 1 Edificio de Periférico (CATD caso	25 abril al 30 de junio de 2024

			fortuito)	
	Servicio de configuración, gestión, monitoreo y visualización del CCTV	1 Servicio	21 Juntas Electorales Distritales, 1 Edificio de Méndez (CCV), 1 Edificio de Periférico (CATD caso fortuito)	25 abril al 30 de junio de 2024
	Suministro de cables HDMI de 20 metros.	5 cables HDMI	Edificio de Méndez (CCV)	25 abril al 30 de junio de 2024
	Suministro de cables HDMI de 1.8 metros.	80 cables HDMI	Edificio de Méndez (CCV)	25 abril al 30 de junio de 2024
	Instalación y desmantelamiento de Equipo de grabación NVR (Propiedad del IEPCT).	23 NVR	21 Juntas Electorales Distritales 1 Centro de Captura y Verificación CCV 1 Edificio Sede (Periférico)	25 abril al 30 de junio de 2024
	Instalación y desmantelamiento de 84 Cámaras IP Tipo Bala deberá incluir cableado UTP Cat 5e para su implementación (Propiedad del IEPCT).	1 Servicio	84 son para las 21 Juntas Electorales Distritales	25 abril al 30 de junio de 2024

	Servicio de renta de 2 pantalla de 43" y 2 equipos de monitoreo.	1 Servicio	Oficinas Centrales	25 abril al 30 de junio de 2024
	Personal de operación de monitoreo.	2 Monitoristas	Oficinas Centrales	25 abril al 30 de junio de 2024

FICHA TECNICA DEL LOTE 2

Características Técnicas	
Servicio de renta de instalación de cámaras de circuito cerrado de CCTV y grabación en sitio	Servicio de arrendamiento para solución de **CCTV** para las Juntas Electorales Distritales, Edificio de Méndez (CCV), Edificio de Periférico CATD para el IEPC Tabasco, deberá cumplir con los siguientes elementos: El proveedor deberá suministrar, instalar y desmantelar **49 cámaras IP** tipo bala donde 42 son para las 21 Juntas Electorales Distritales, 2 para Edificio de Periférico CATD y 5 Edificio de Méndez (CCV) con las siguientes características: Deberá contar con una resolución de 2 megapixeles, distancia de alcance de 30 metros por medio de ir, lente de 2.8 mm, equipo con resistencia para el exterior ip67, soporte memoria micro sd de hasta 128 gb clase 10 o superior, rango dinámico amplio de al menos 100 db, deberá contar con soporte de video analíticos integrados de detección de rostros, deberá contar con streaming de video de tipo: principal de 50 hz: 25fps (1920 ×1080,1280 ×960,1280 ×720) / 60 hz: 30fps (1920 × 1080,1280 × 960,1280 ×720), secundario 50 hz: 25fps (640 × 480, 640 × 360, 320 × 240) / 60 hz: 30 fps (640 × 480, 640× 360, 320 × 240), tercer 50hz: 25fps (1920 × 1080, 1280×720, 640 × 360, 352 × 288) / 60hz: 30fps (1920 × 1080, 1280×720, 640 × 360, 352 × 240), estándares de compresión de video soportados h.264/h.264+/h.265/h.265+, debera contar con conexión de red 10/100 ethernet, soporte de hasta 32 idiomas para control web por parte del cliente, soporte de los siguientes protocolos tcp/ip, icmp, http, https, dhcp, dns, rtp, rtsp, rtcp, ntp, igmp, qos, udp, alimentación eléctrica por medio de conexión de 12 vdc +- 25% / poe (802.3af, 36v to 57v), 0.2a a 0.1a, max. 7.5w, rotación de dia/noche dia/noche/automático/programado, deberá contar con una garantía de 2 años en sitio, deberá incluir cableado CAT 5e para su instalación y su registro de protección para los conectores. El proveedor deberá suministrar, instalar y desmantelar 23 gabinetes para las 21 Juntas Electorales Distritales, Edificio de Méndez (CCV), Edificio de Periférico (CATD caso fortuito) montaje en pared con puerta de cristal templado con un cuerpo fijo de rack de 19" de 6 unidades de rack color negro semi-mate aplicada por proceso electrostático horneado de 5 pasos: desengrasado, enjuague, fosfato de hierro, enjuague y sellado pintura base poliéster, deberá incluir chapa de seguridad en puerta la puerta deberá ser desmontable y se podrá cambiar el sentido de apertura con cuerpo principal soldado para asegurar estabilidad la ventana de cristal deberá ser resistente a impactos con un año de garantía con el fabricante. El proveedor deberá suministrar, instalar y desmantelar 23 UPS para las 21 Juntas Electorales Distritales, Edificio de Méndez (CCV), y Edificio de Periférico (CATD caso fortuito) factor forma rack de 1 unidad, con un tiempo mínimo de 45 minutos de respaldo

	a media carga, con al menos 4 tomacorrientes en batería y sobretensiones, además de 2 tomacorrientes para sobretensiones, el tiempo mínimo de recarga de batería sería de 6 horas, con conector de entrada tipo nema 5-15p, con un tiempo de transferencia automática de 8ms, deberá tener un panel LCD, alarmas audibles en: modo de batería, falla de sobrecarga de batería baja, deberá tener una garantía de 3 años por parte del fabricante. Deberá incluir el servicio de configuración para CCTV para la gestión, monitoreo y visualización de las 21 juntas electorales distritales, edificio periférico y el CCV de Méndez con capacidad para la grabación remota, local y la integración de estos desde el Instituto Electoral y de Participación Ciudadana de Tabasco. Deberá suministrar 5 cables hdmi de 20 metros minimo que soporte video 3d y hasta resoluciones hd 4k x 2k (4096 x 2160) con conexiones hdmi macho a macho de 19 pines bañados en oro de 24k que soporte anchos de banda de alta velocidad 10.2 gigabit/segundo, 340 mhz, soportando las siguientes resoluciones 480i, 480p, 720p, 1080p, 1600i, 1600p, soporta 4k x 2k (3840 x 2160, 4096 x 2160) especificaciones v1.4 con soporte de 120 hz / 240 hz / 480 hz con compatibilidad al 100% con dolby true hd, dts-hd master audio, sony playstation 3, blue-ray hd dvd, hd-dvd con garantia de 1 año por parte del fabricante. Deberá suministrar 80 cables HDMI de alta velocidad de 1.8 mts., con conexiones HDMI macho a macho, color negro, que soporte resoluciones de hasta FHD 1080p. La solución de sistema **CCTV** deberá incluir instalación y desmantelamiento (final del proceso fecha estimada 30 de junio) un NVR en cada una de las 21 Juntas Electorales Distritales, 1 NVR en el Edificio de Periférico CATD, 1 NVR en el Edificio Méndez CCV (Centro de Captura y Verificación), estos equipos serán proporcionados por el Instituto Electoral al proveedor para su instalación y desmantelamiento La solución de sistema **CCTV** deberá instalar y desmantelar (final del proceso fecha estimada 30 de junio) 84 cámaras de CCTV (4 en cada de una de las 21 Juntas Electorales Distritales), estos equipos serán proporcionados por el Instituto Electoral al proveedor para su instalación y desmantelamiento, de igual manera el proveedor deberá incluir cableado CAT 5e para su instalación y su registro de protección para los conectores. Se deberá incluir: instalación, configuración y puesta en marcha de la solución de CCTV en sitio propuesta anteriormente en esta presente ficha técnica. Se deberá presentar carta de distribuidor autorizado por parte de la marca. Se deberá considerar el mantenimiento, soporte y asistencia remota en cada sitio para la adecuada prestación del servicio solicitado.
Servicio de renta de pantalla y equipo de monitoreo	Se deberá incluir 4 pantallas de 43 pulgadas o superior para los monitoristas con las siguientes características mínimas: resolución full hd 1920 x 1080, pantalla plana, velocidad de refresco de 60hz, relación de aspecto de 16x9, soporte de puerto de red rj45 ethernet, garantía de 1 año, 2 puertos HDMI, 1 puerto USB, entrada VGA opcional, soporte para montaje vesa, reproductor de medios por USB, WI-FI integrado. Se deberá incluir 2 estaciones de trabajo para los monitoristas con las siguientes características mínimas: procesador intel xeon e2274g (8m cache, 4 ghz con turbo 4.9 ghz), 16 gb ram ddr4 2666 mhz con capacidad máxima de 64 gb ddr4, disco duro 256 gb ssd m.2, disco duro de 1 tb 7200 rpm, tarjeta de red 10/100/1000 base-t, 2 puertos

	usb 2.0, 6 puertos usb 3.0 tipo a, 1 puerto usb 3.0 tipo c, 2 puertos display port, 1 salida de auricular, tarjeta de video nvidia quadro p620 con 2 gb, windows 11 profesional en español, debera contar con 3 años de garantía en sitio. Se deberá considerar el mantenimiento, soporte y asistencia remota en sitio para la adecuada prestación del servicio solicitado.
Personal de operación de monitoreo	El proveedor para garantizar el servicio de monitoreo deberá integrar en su propuesta los elementos siguientes: 2 técnicos monitoristas con equipo de comunicación celular para reporte de cualquier evento de importancia crítica y/o de emergencia, se deberá cubrir un horario nocturno de 22:00 horas a 8:00 horas, al finalizar la jornada de trabajo del día se deberá entregar un reporte de actividades de lo sucedido en el tiempo laborado, los técnicos monitoristas no tendrán funciones de control de asistencia ni reporte de entrada y salida de personal, las responsabilidades de los monitoristas es identificar de inmediato (o en el menor tiempo posible), cualquier situación que ponga en riesgo la seguridad de los domicilios. informar a los números telefónicos que el instituto designe los acontecimientos de riesgo de seguridad.

UBICACIÓN GEOGRAFICA

JUNTAS ELECTORALES DISTRITALES			
No.	Municipio	Domicilio	Coordenada Geodésica
1	Cárdenas	Calle Caoba número 221 esq. Calle Ceiba, Fracc. Los Reyes Loma Alta, Cárdenas, Tabasco.	17.987398981484727, -93.39034505630875
2	Cárdenas	27 de febrero número 147, Col. Pueblo Nuevo, Cárdenas, Tabasco.	17.997224, -93.380146
3	Cárdenas	Calle Guadalupe Victoria esq. Venustiano Carranza s/n, Col. Centro, Cárdenas, Tabasco.	17.996722, -93.372699
4	Centla	Calle Benito Juárez Num. 406 Col. Centro, Frontera, Centla, Tabasco.	18.528326, -92.651923
5	Centro	Carretera a Ixtacomitán 1ra. Sección Km. 2.5 S/N Ra. Ixtacomitán 3a Sección, Villahermosa, Tabasco.	17.949185, -92.938595
6	Centro	Calle Revolución No. 48 , Villa Macultepec, C.P. 86250 Centro, Tabasco.	18.1390494, -92.8576822
7	Centro	Calle Sindicato de Economía Núm. 210, Col. Adolfo López Mateos, Villahermosa, Centro, Tabasco.	17.999580, - 92.930194
8	Centro	Calle Alameda Núm. 8, Colonia Miguel Hidalgo, C.P. 86128 Villahermosa, Centro, Tabasco.	17.975474364818382, -92.97215775692511
9	Centro	C. Heroico Colegio Militar Núm. 125, Col. Primero de Mayo, C.P. 86100 Villahermosa, Tabasco.	17.978378, -92.942207
10	Centro	Calle Francisco I. Madero Núm. 202, Esquina Ausencio G. Cruz, Villa Playas del Rosario, Centro, Tabasco.	17.854460, -92.930267
11	Comalcalco	Calle Cacao Núm. 100, Col. las Rosas, Comalcalco, Tabasco.	18.257223, -93.212733
12	Comalcalco	Blvd. Leandro Rovirosa Wade Núm. 459, Colonia San Francisco C.P. 86330 Comalcalco, Tabasco.	18.269911, -93.226852

13	Cunduacán	Calle Playa del Rosario s/n, Fracc. Playa Azul, Col. Centro, Cunduacán; Tabasco.	18.062436, -93.173677
14	Emiliano Zapata	Calle Simón Sarlat Núm. 20, entre G. Méndez y Morelos , Col. Centro, E. Zapata, Tabasco.	17.743042, -91.764382
15	Huimanguillo	Av. De la Juventud Núm. 20, Col. Magisterial, Huimanguillo, Tabasco.	17.813667, -93.398661
16	Macuspana	Prol. Agustín Díaz del Castillo, Esq. Circunvalación, Macuspana, Tabasco.	17.753509, -92.588919
17	Jalpa de Méndez	Calle del Retén No. 4, Poblado Amatitán, Jalpa de Méndez, Tabasco.	18.1767943, -93.0804386
18	Nacajuca	Calle Crisanto Palma Núm 26, Col. Centro, Nacajuca, Tabasco.	18.16575793153521, -93.0181401729923
19	Paraíso	Calle Desiderio G. Rosado Sastré S/N, Col. Guanajai, C.P. 86607 Paraíso, Tabasco.	18.411712, -93.204267
20	Teapa	Av. Carlos A. Madrazo No. 190, Col. Sierra Arroyo, Teapa, Tabasco.	17.562814, -92.946193
21	Tenosique	C. Chichén Itzá S/N Fraccionamiento Pomona, Tenosique de Pino Suárez, Tabasco.	17.455857, -91.426581

No.	Municipio	Domicilio	Coordenada Geodésica
22	Centro	C. Eusebio Castillo 747, Nueva Villahermosa, 86000 Villahermosa, Tab.	17.994018835296785, -92.92081780739834

No.	Municipio	Domicilio	Coordenada Geodésica
23	Centro	Av. Gregorio Méndez 716, Juan Álvarez y Eusebio Castillo, Fracc. Arboledas, Villahermosa, Centro, Tabasco	17.993233,-92.919256
24	Centro	Av. Periférico Carlos Pellicer Cámara No. 1206 Col. Tamulté de las Barrancas, Villahermosa, Tabasco	17.966291, -92.951558

ATENTAMENTE

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
IEPC TABASCO
COMITÉ DE COMPRAS

Lic. Javier García Rodríguez
Presidente del Comité de Compras del Instituto Electoral y de Participación Ciudadana de Tabasco

"ANEXO 6"

CUMPLIMIENTO EN CANTIDADES Y CARACTERÍSTICAS DE LOS SERVICIOS

ARTÍCULO 53 DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y PRESTACIÓN DE SERVICIOS DEL ESTADO DE TABASCO

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Yo _____ en mi carácter de representante legal de la empresa denominada _____, declaro bajo protesta de decir verdad lo siguiente:

Que los servicios ofertados cumplen cabalmente con las cantidades, características y especificaciones que se describen en el **"Anexo 5"** de las bases de la Licitación Pública Estatal N° _____, relativa a la contratación de Servicios Integrales De Infraestructura De Cómputo, por lo que mi representada se compromete ante el Instituto Electoral y de Participación Ciudadana de Tabasco a responder por:

a) Los defectos; y
b) Vicios ocultos en los bienes en la prestación de los servicios, así como de cualquier otra responsabilidad en que incurra conforme a los términos señalados en el contrato respectivo.

Lo anterior, en cumplimiento con lo estipulado en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco.

PROTESTO LO NECESARIO

_____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

"ANEXO 7"

FORMATO DE OFERTA ECONÓMICA

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Lote/partida	Cantidad solicitada	Unidad	Descripción de los servicios	Precio Unitario	Importe
				Subtotal	
				IVA	
				Total	

PROTESTO LO NECESARIO

_____

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

NOTA: Los descuentos ofrecidos, deberán incluirse en los precios unitarios.

El presente formato podrá ser reproducido por cada participante en la manera que estime conveniente, debiendo respetar su contenido, preferentemente, en el orden indicado.

"ANEXO 8"

DECLARACIONES SOBRE LA GARANTÍA DE CUMPLIMIENTO (FIANZA)

POR: *(NOMBRE DE LA EMPRESA)*
DIRECCIÓN: _____

ANTE: INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO.
DIRECCIÓN: EUSEBIO CASTILLO 747, COL. CENTRO, VILLAHERMOSA, TABASCO, C.P. 86000.

ADQUISICIÓN RELATIVA A LA CONTRATACIÓN DE SERVICIOS INTEGRALES DE INFRAESTRUCTURA DE CÓMPUTO, BAJO LOS LINEAMIENTOS E INDICACIONES QUE DETERMINE EL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO. PARA GARANTIZAR POR *(NOMBRE DE LA EMPRESA)*, EL DEBIDO CUMPLIMIENTO DE LAS OBLIGACIONES CONTENIDAS EN EL CONTRATO NÚMERO _____ DE FECHA __ DE ____ DE 2023, POR UN IMPORTE TOTAL DE $_____ (_____ PESOS 00/100 M.N.), EL CUAL INCLUYE EL IMPUESTO AL VALOR AGREGADO. LA PRESENTE FIANZA SE EXPIDE DE ACUERDO CON EL CONTRATO DE REFERENCIA, POR EL 20% DEL MONTO TOTAL DEL MISMO, CON UNA VIGENCIA DEL ___ DE ___ DE ____ AL ___ DE ___ DE ____.

NOMBRE DE LA AFIANZADORA, EXPRESAMENTE DECLARA:

I. QUE LA FIANZA SE OTORGA PARA GARANTIZAR TODAS Y CADA UNA DE LAS OBLIGACIONES CONTENIDAS EN EL CONTRATO ANTES SEÑALADO;
II. QUE LA AFIANZADORA SE SOMETE EXPRESAMENTE A PROCEDIMIENTOS ESPECIALES ESTABLECIDOS EN EL ARTÍCULO 282 DE LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS PARA LA EFECTIVIDAD DE LAS FIANZAS, AÚN PARA EL CASO DE QUE PROCEDIERA EL COBRO DE INTERESES;
III. QUE LA AFIANZADORA ACEPTA EXPRESAMENTE SOMETERSE A LOS PROCEDIMIENTOS DE EJECUCIÓN PREVISTOS EN LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS PARA LA EFECTIVIDAD DE LAS FIANZAS;
IV. QUE LA FIANZA ESTARÁ VIGENTE DURANTE LA SUBSTANCIACIÓN DE TODOS LOS RECURSOS LEGALES O JUICIOS QUE SE INTERPONGAN Y HASTA EN TANTO SE DICTE RESOLUCIÓN DEFINITIVA POR AUTORIDAD COMPETENTE;
V. QUE LA PÓLIZA DE FIANZA NO SE SUJETARÁ A LO PREVISTO EN EL ARTÍCULO 174 DE LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS, POR LO QUE LA FIGURA JURÍDICA DE CADUCIDAD NO LE SERÁ APLICADA;
VI. EN CASO DE OTORGAMIENTO DE PRÓRROGA O ESPERA DERIVADA DE LA FORMALIZACIÓN DE CONVENIOS DE AMPLIACIÓN AL MONTO O EL PLAZO DE EJECUCIÓN DEL CONTRATO, SE DEBERÁ OBTENER LA MODIFICACIÓN DE LA FIANZA EN UN PLAZO NO MAYOR DE DIEZ DÍAS NATURALES A LA NOTIFICACIÓN QUE SE HAGA AL "PROVEEDOR" POR ESCRITO, POR PARTE DEL "INSTITUTO";
VII. QUE PARA LIBERAR LA FIANZA SERÁ REQUISITO INDISPENSABLE LA MANIFESTACIÓN EXPRESA Y POR ESCRITO DEL "PROVEEDOR" AL "INSTITUTO"; Y
VIII. QUE LAS PARTES CONVIENEN QUE LA PÓLIZA ES DE CARÁCTER INDIVISIBLE.

---------- FIN DE TEXTO ----------

"ANEXO 9"

CALENDARIO DE ACTOS

ACTOS	FECHA	HORARIO	HORARIO DE REGISTRO
Publicación de la Convocatoria en el Periódico Oficial del Estado, Sistema CompraNet Tabasco y en la página institucional	**23/Marzo/2024**		
Venta de bases	**23 al 27 de Marzo de 2024**	**lunes a viernes 10:00 a 15:00 hrs.**	
Fecha límite para recepcionar preguntas	**29/Marzo/2024**	**hasta las 19:00 hrs.**	
Junta de Aclaraciones	**01/Abril/2024**	**10:00 hrs.**	**09:30 A 09:59 hrs.**
Acto de Presentación de Propuestas Técnicas y Económicas, y Apertura de Propuestas Técnicas	**08/Abril/2024**	**10:00 hrs.**	**09:30 A 09:59 hrs.**
Acto de Lectura de Fallo Técnico, Apertura de Propuestas Económicas y Fallo de la Licitación	**09/Abril/2024**	**10:00 hrs.**	**09:30 A 09:59 hrs.**

"ANEXO 10"

FORMATO PARA LA PRESENTACIÓN DE PREGUNTAS A LA CONVOCANTE

Villahermosa, Tabasco a _____ de _____.

LIC. JAVIER GARCÍA RODRÍGUEZ
PRESIDENTE DEL COMITÉ DE COMPRAS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
P R E S E N T E.

Por medio del presente, me permito solicitar las aclaraciones de las siguientes dudas referentes a la Licitación Pública Estatal N° _____, relativa a la contratación de _____.

De carácter administrativo y/o legal:

PREGUNTAS
1.-
2.-

De carácter técnico:

PREGUNTAS
1.-
2.-

PROTESTO LO NECESARIO

_____

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA