REPÚBLICA DOMINICANA

MINNISTERIO DE HACIENDA

"Año del Fomento de las Exportaciones"

PLIEGO DE CONDICIONES ESPECÍFICAS PARA COMPRA DE BIENES Y SERVICIOS CONEXOS

Ampliación de las Soluciones de Web Application Firewall, Application Delivery, Balanceo de Aplicaciones y Protección de DDOS; Gateways de Manejo y Control de Seguridad Integrada y Software de Seguridad para la Infraestructura de Virtualización del Ministerio de Hacienda.

Procedimiento de Excepción por proveedor único
PAFI-CCC-PEPU-2018-0010

Santo Domingo, Distrito Nacional
República Dominicana
Septiembre, 2018

TABLA DE CONTENIDO

GENERALIDADES

Prefacio

Este modelo estándar de Pliego de Condiciones Específicas para Compras y Contrataciones de Bienes y/o Servicios conexos, ha sido elaborado por la Dirección General de Contrataciones Públicas, para ser utilizado en los Procedimientos de Licitaciones regidos por la Ley No. 340-06, de fecha dieciocho (18) de agosto del dos mil seis (2006), sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, su modificatoria contenida en la Ley No. 449-06, de fecha seis (06) de diciembre del dos mil seis (2006), y su Reglamento de Aplicación emitido mediante el Decreto No. 543-12 de fecha seis (6) de septiembre de dos mil doce (2012).

A continuación se incluye una breve descripción de su contenido.

PARTE 1 – PROCEDIMIENTOS DE PROCEDIMIENTO DE EXCEPCIÓN DE PROVEEDOR ÚNICO

Sección I. Instrucciones a los Oferentes (IAO)

Esta sección proporciona información para asistir a los Oferentes en la preparación de sus Ofertas. También incluye información sobre la presentación, apertura y evaluación de las ofertas y la adjudicación de los contratos. Las disposiciones de la Sección I son de uso estándar y obligatorio en todos los procedimientos de Excepción de Proveedor Único para Compras y Contrataciones de Bienes y/o Servicios conexos regidos por la Ley No. 340-06 sobre Compras y Contrataciones con modificaciones de Ley No. 449-06 y su Reglamento de aplicación aprobado mediante Decreto No. 543-12.

Sección II. Datos del Procedimiento de Excepción de Proveedor Único (DDPEPU)

Esta sección contiene disposiciones específicas para cada Compra y Contratación de Bienes y/o Servicios conexos, y complementa la Sección I, Instrucciones a los Oferentes.

Sección III. Apertura y Validación de Ofertas

Esta sección incluye el procedimiento de apertura y validación de Ofertas, Técnicas y Económicas, incluye los criterios de evaluación y el procedimiento de Estudio de Precios.

Sección IV. Adjudicación

Esta sección incluye los Criterios de Adjudicación y el Procedimiento para Adjudicaciones Posteriores.

PARTE 2 - CONTRATO

Sección V. Disposiciones sobre los Contrato

Esta sección incluye el Contrato, el cual, una vez perfeccionado no deberá ser modificado, salvo los aspectos a incluir de las correcciones o modificaciones que se hubiesen hecho a la oferta seleccionada y que están permitidas bajo las Instrucciones a los Oferentes y las Condiciones Generales del Contrato.

Incluye las cláusulas generales y específicas que deberán incluirse en todos los contratos.

PARTE 3 – ENTREGA Y RECEPCION

Sección VI. Recepción de los Productos

Esta sección incluye los requisitos de la entrega, la recepción provisional y definitiva de los bienes, así como las obligaciones del proveedor.

Sección VII. Formularios

Esta sección contiene los formularios de información sobre el oferente, presentación de oferta y garantías que el oferente deberá presentar conjuntamente con la oferta.

PARTE I
PROCEDIMIENTOS DE EXCEPCIÓN DE PROVEEDOR ÚNICO

Sección I
Instrucciones a los Oferentes (IAO)

1.1 Antecedentes

En el año 2017 el Ministerio de Hacienda, apoyado en una evaluación interna sobre su infraestructura tecnológica y la de algunas de sus dependencias, en la que se identificó la necesidad de realizar una readecuación de su Centro de Datos, definió unas iniciativas estratégicas dentro del foco de Tecnología de la Información, entre las cuales se encuentran la Actualización Tecnológica y el Fortalecimiento Institucional.

Para apoyar las citadas iniciativas, el Ministerio de Hacienda proyectó una serie de inversiones orientadas a la adquisición y desarrollo de importantes sistemas de información, que requieren de una alta capacidad adicional de recursos de computación, en términos de almacenamiento, conectividad, seguridad y alta disponibilidad. Por lo que requiere ampliar las capacidades de sus recursos actuales, a fin de suplir la demanda.

1.2 Objetivos y Alcance

El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras, que deseen participar en el Procedimiento de Excepción de Proveedor Único para la compra de **Ampliación de las Soluciones de Web Application Firewall, Application Delivery, Balanceo de Aplicaciones y Protección de DDOS; Gateways de Manejo y Control de Seguridad Integrada y Software de Seguridad para la Infraestructura de Virtualización del Ministerio de Hacienda,** llevada a cabo por **el Programa de Administración Financiera Integrada(PAFI) del Ministerio de Hacienda** **(Referencia: PAFI-CCC-PEPU-2018-0010[1]).**

Este documento constituye la base para la preparación de las Ofertas. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en el presente Pliego de Condiciones Específicas o presenta una información que no se ajuste sustancialmente en todos sus aspectos al mismo, el riesgo estará a su cargo y el resultado podrá ser el rechazo de su Propuesta.

1.3 Definiciones e Interpretaciones

A los efectos de este Pliego de Condiciones Específicas, las palabras y expresiones que se inician con letra mayúscula y que se citan a continuación tienen el siguiente significado:

[1] **La referencia corresponde al nombre de la institución- Comité de Compras y Contrataciones - Procedimiento de Excepción de Proveedor Único- Año- número secuencial de procedimientos llevados a cabo.**

Adjudicatario: Oferente/Proponente a quien se le adjudica el Contrato u Orden de Compra.

Bienes: Productos elaborados a partir de materias primas, consumibles para el funcionamiento de los Entes Estatales.

Caso Fortuito: Acontecimiento que no ha podido preverse, o que previsto no ha podido evitarse, por ser extraño a la voluntad de las personas.

Circular: Aclaración que el Comité de Compras y Contrataciones emite de oficio o para dar respuesta a las consultas planteadas por los Oferentes/Proponentes con relación al contenido del Pliego de Condiciones, formularios, otra Circular o anexos, y que se hace de conocimiento de todos los Oferentes/Proponentes.

Comité de Compras y Contrataciones: Órgano Administrativo de carácter permanente responsable de la designación de los peritos que elaborarán las especificaciones técnicas del bien a adquirir y del servicio u obra a contratar, la aprobación de los Pliegos de Condiciones Específicas, del Procedimiento de Selección y el dictamen emitido por los peritos designados para evaluar ofertas.

Compromiso de Confidencialidad: Documento suscrito por el Oferente/Proponente para recibir información del Procedimiento de Excepción de Proveedor Único.

Consorcio: Uniones temporales de empresas que sin constituir una nueva persona jurídica se organizan para participar en un procedimiento de contratación.

Consulta: Comunicación escrita, remitida por un Oferente/Proponente conforme al procedimiento establecido y recibida por el Comité de Compras y Contrataciones, solicitando aclaración, interpretación o modificación sobre aspectos relacionados exclusivamente con el Pliego de Condiciones Específicas.

Contrato: Documento suscrito entre la institución y el Adjudicatario elaborado de conformidad con los requerimientos establecidos en el Pliego de Condiciones Específicas y en la Ley.

Credenciales: Documentos que demuestran las calificaciones profesionales y técnicas de un Oferente/Proponente, presentados como parte de la Oferta Técnica y en la forma establecida en el Pliego de Condiciones Específicas, para ser evaluados y calificados por los peritos, lo que posteriormente pasa a la aprobación del Comité de Compras y Contrataciones de la entidad contratante, con el fin de seleccionar los Proponentes Habilitados, para la apertura de su Oferta Económica Sobre B.

Cronograma de Actividades: Cronología del Proceso de Excepción de Proveedor Único.

Día: Significa días calendarios.

Días Hábiles: Significa día sin contar los sábados, domingos ni días feriados.

Enmienda: Comunicación escrita, emitida por el Comité de Compras y Contrataciones, con el fin de modificar el contenido del Pliego de Condiciones Específicas, formularios, anexos u otra Enmienda y que se hace de conocimiento de todos los Oferentes/Proponentes.

Entidad Contratante: El organismo, órgano o dependencia del sector público, del ámbito de aplicación de la Ley No. 340-06, que ha llevado a cabo un proceso contractual y celebra un Contrato.

Estado: Estado Dominicano.

Fichas Técnicas: Documentos contentivos de las Especificaciones Técnicas requeridas por la Entidad Contratante.

Fuerza Mayor: Cualquier evento o situación que escapen al control de la Entidad Contratante, imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, epidemias, guerras, actos de terroristas, huelgas, fuegos, explosiones, temblores de tierra, catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo.

Interesado: Cualquier persona natural o jurídica que tenga interés en cualquier procedimiento de compras que se esté llevando a cabo.

Líder del Consorcio: Persona natural o jurídica del Consorcio que ha sido designada como tal.

Máxima Autoridad Ejecutiva: El titular o el representante legal de la Entidad Contratante o quien tenga la autorización para celebrar Contrato.

Notificación de la Adjudicación: Notificación escrita al Adjudicatario y a los demás participantes sobre los resultados finales del Procedimiento de Excepción de Proveedor Único, dentro de un plazo de **cinco (05) días hábiles** contados a partir del Acto de Adjudicación.

Oferta Económica: Precio fijado por el Oferente en su Propuesta.

Oferta Técnica: Especificaciones de carácter técnico-legal de los Bienes y Servicios conexos a ser adquiridos.

Oferente/Proponente: Persona natural o jurídica legalmente capacitada para participar en el proceso de compra.

Oferente/Proponente Habilitado: Aquel que participa en el proceso de Excepción de Proveedor Único y resulta Conforme en la fase de Evaluación Técnica del Proceso.

PAFI: Es el Programa de Administración Financiera Integrada del Ministerio de Hacienda, el cual está en proceso interno de pasar a Dirección de Área con una nueva denominación de Dirección de Administración Financiera Integrada (DAFI).

Peritos: Funcionarios expertos en la materia del proceso llevado a cabo, de la Entidad Contratante, de otra entidad pública o contratados para el efecto y que colaborarán asesorando, analizando y evaluando propuestas, confeccionando los informes que contengan los resultados y sirvan de sustento para las decisiones que deba adoptar el Comité de Compras y Contrataciones.

Prácticas de Colusión: Es un acuerdo entre dos o más partes, diseñado para obtener un propósito impropio, incluyendo el influenciar inapropiadamente la actuación de otra parte.

Prácticas Coercitivas: Es dañar o perjudicar, o amenazar con dañar o perjudicar directa o indirectamente a cualquier parte, o a sus propiedades para influenciar inapropiadamente la actuación de una parte.

Prácticas Obstructivas: Es destruir, falsificar, alterar u ocultar en forma deliberada pruebas importantes respecto de su participación en un proceso de compra o incidir en la investigación o formular declaraciones farsas a los investigadores con la intensión de impedir sustancialmente una investigación de la Entidad Contratante referente a acusaciones sobre prácticas corruptas, fraudulentas, coercitivas, o colusorias y/o amenazar, acosar o intimidar a una parte con el propósito de impedir que dicha parte revele lo que sabe acerca de asuntos pertinentes a la investigación, o que lleve adelante la investigación, o la ejecución de un Contrato.

Procedimiento de Excepción de Proveedor Único: Procesos de adquisición de bienes o servicios que sólo puedan ser suplidos por una determinada persona natural o jurídica. En caso de entregas adicionales del proveedor original que tengan por objeto ser utilizadas como repuestos, ampliaciones o servicios continuos para equipos existentes, programas de cómputos, servicios o instalaciones. Cuando un cambio de proveedor obligue a la Entidad a adquirir mercancías o servicios que no cumplan con los requisitos de compatibilidad con los equipos, programas de cómputos, servicios o instalaciones existentes o la utilización de patentes o marcas exclusivas o tecnologías que no admitan otras alternativas técnicas.

Pliego de Condiciones Específicas: Documento que contiene todas las condiciones por las que habrán de regirse las partes en el presente Procedimiento de Excepción de Proveedor Único.

Proveedor: Oferente/Proponente que habiendo participado en el Procedimiento de Excepción de Proveedor Único, resulta adjudicatario del contrato y suministra productos de acuerdo a los Pliegos de Condiciones Específicas.

Representante Legal: Persona física o natural acreditada como tal por el Oferente/ Proponente.

Reporte de Lugares Ocupados: Formulario que contiene los precios ofertados en el procedimiento, organizados de menor a mayor.

Resolución de la Adjudicación: Acto Administrativo mediante el cual el Comité de Compras y Contrataciones procede a la Adjudicación al/los oferente(s) del o los Contratos objeto del procedimiento de compra o contratación

Sobre: Paquete que contiene las credenciales del Oferente/Proponente y las Propuestas Técnicas o Económicas.

Unidad Operativa de Compras y Contrataciones (UOCC): Unidad encargada de la parte operativa de los procedimientos de Compras y Contrataciones.

Para la interpretación del presente Pliego de Condiciones Específicas:

- Las palabras o designaciones en singular deben entenderse igualmente al plural y viceversa, cuando la interpretación de los textos escritos lo requiera.
- El término **"por escrito"** significa una comunicación escrita con prueba de recepción.
- Toda indicación a capítulo, numeral, inciso, Circular, Enmienda, formulario o anexo se entiende referida a la expresión correspondiente de este Pliego de Condiciones Específicas, salvo indicación expresa en contrario. Los títulos de capítulos, formularios y anexos son utilizados exclusivamente a efectos indicativos y no afectarán su interpretación.
- Las palabras que se inician en mayúscula y que no se encuentran definidas en este documento se interpretarán de acuerdo a las normas legales dominicanas.
- Toda cláusula imprecisa, ambigua, contradictoria u oscura a criterio de la Entidad Contratante, se interpretará en el sentido más favorable a ésta.

1.4 Idioma

El idioma oficial del presente Procedimiento de Excepción de Proveedor Único es el español, por tanto, toda la correspondencia y documentos generados durante el procedimiento que intercambien el Oferente/Proponente y el Comité de Compras y Contrataciones deberán ser presentados en este idioma o, de encontrarse en idioma distinto, deberán contar con la traducción al español realizada por un intérprete judicial debidamente autorizado.

1.5 Precio de la Oferta

Los precios cotizados por el Oferente en el Formulario de Presentación de Oferta Económica deberán ajustarse a los requerimientos que se indican a continuación.

Todos los lotes y/o artículos deberán enumerarse y cotizarse por separado en el Formulario de Presentación de Oferta Económica. Si un formulario de Oferta Económica detalla artículos pero no los cotiza, se asumirá que está incluido en la Oferta. Asimismo, cuando algún lote o artículo no aparezca en el formulario de Oferta Económica se asumirá de igual manera, que está incluido en la Oferta.

El desglose de los componentes de los precios se requiere con el único propósito de facilitar a la Entidad Contratante la comparación de las Ofertas.

El precio cotizado en el formulario de Presentación de la Oferta Económica deberá ser el precio total de la oferta, excluyendo cualquier descuento que se ofrezca.

Los precios cotizados por el Oferente serán fijos durante la ejecución del Contrato y no estarán sujetos a ninguna variación por ningún motivo, salvo lo establecido en los **Datos del Procedimiento de Excepción de Proveedor Único (DDPEPU).**

1.6 Moneda de la Oferta

El precio en la Oferta deberá estar expresado en moneda nacional, (Pesos Dominicanos, RD$), a excepción de los Contratos de suministros desde el exterior, en los que podrá expresarse en la moneda del país de origen de los mismos.

De ser así, el importe de la oferta se calculará sobre la base del tipo de cambio vendedor del BANCO CENTRAL DE LA REPÚBLICA DOMINICANA vigente al cierre del día anterior a la fecha de recepción de ofertas.

1.7 Normativa Aplicable

El proceso de Excepción de Proveedor Único, el Contrato y su posterior ejecución se regirán por la Constitución de la República Dominicana, Ley No. 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, de fecha dieciocho (18) de agosto del 2006, su modificatoria contenida en la Ley No. 449-06 de fecha seis (06) de diciembre del 2006; y su Reglamento de Aplicación emitido mediante el Decreto No. 543-12, de fecha Seis (06) de septiembre del 2012, por las normas que se dicten en el marco de la misma, así como por el presente Pliego de Condiciones y por el Contrato a intervenir.

Todos los documentos que integran el Contrato serán considerados como recíprocamente explicativos.

Para la aplicación de la norma, su interpretación o resolución de conflictos o controversias, se seguirá el siguiente orden de prelación:

1) La Constitución de la República Dominicana;
2) La Ley No. 340-06, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, de fecha 18 de agosto del 2006 y su modificatoria contenida en la Ley No. 449-06 de fecha seis (06) de diciembre del 2006;
3) El Reglamento de Aplicación de la Ley No. 340-06, emitido mediante el Decreto No. 543-12, de fecha Seis (06) de septiembre del 2012;
4) Decreto No. 164-13 para fomentar la producción nacional y el fortalecimiento competitivo de las MIPYMES de fecha diez (10) de junio del 2013.
5) Resolución No. 33-16, de fecha veintiséis (26) de abril del 2016 sobre fraccionamiento, actividad comercial del registro de proveedores y rubro emitida por la Dirección de Contrataciones Públicas.
6) Resolución 154-16, de fecha veinticinco (25) de mayo del 2016 sobre las consultas en línea emitida por el Ministerio de Hacienda.
7) Las políticas emitidas por el Órgano Rector.
8) El Pliego de Condiciones Específicas;
9) La Oferta y las muestras que se hubieren acompañado;
10) La Adjudicación;
11) El Contrato;
12) La Orden de Compra.

1.8 Competencia Judicial

Todo litigio, controversia o reclamación resultante de este documento y/o el o los Contratos a intervenir, sus incumplimientos, interpretaciones, resoluciones o nulidades serán sometidos al Tribunal Superior Administrativo conforme al procedimiento establecido en la Ley que instituye el Tribunal Superior Administrativo.

1.9 Proceso Arbitral

De común acuerdo entre las partes, podrán acogerse al procedimiento de Arbitraje Comercial de la República Dominicana, de conformidad con las disposiciones de la Ley No. 479-08, de fecha treinta (30) de diciembre del dos mil ocho (2008).

1.10 De la Publicidad

La convocatoria a presentar Ofertas del Procedimiento de Excepción de Proveedor Único, deberá efectuarse mediante la publicación en los portales de la Dirección General de Compras y Contrataciones y el Ministerio de Hacienda..

La comprobación de que en un llamado a Licitación se hubieran omitido los requisitos de publicidad, dará lugar a la cancelación inmediata del procedimiento por parte de la autoridad de aplicación en cualquier estado de trámite en que se encuentre.

1.11 Etapas del Procedimiento de Excepción de Proveedor Único

Las Licitaciones podrán ser de Etapa Única o de Etapas Múltiples.

Etapa Única:
Cuando la comparación de las Ofertas y de la calidad de los Oferentes se realiza en un mismo acto.

Etapa Múltiple:
Cuando la Ofertas Técnicas y las Ofertas Económicas se evalúan en etapas separadas:

Etapa I: Se inicia con el proceso de entrega de los **"Sobres A",** contentivos de las Ofertas Técnicas, acompañadas de las muestras, si procede, en acto público y en presencia de Notario Público. Concluye con la valoración de las Ofertas Técnicas y la Resolución emitida por el Comité de Compras y Contrataciones sobre los resultados del Proceso de Homologación.

Etapa II: Se inicia con la apertura y lectura en acto público y en presencia de Notario Público de las Ofertas Económicas "Sobre B", que se mantenían en custodia y que resultaron habilitados en la primera etapa del procedimiento, y concluye con la Resolución de Adjudicación a los Oferentes/Proponentes.

1.12 Órgano de Contratación

El órgano administrativo competente para la contratación de los Bienes y Servicios conexos a ser adquiridos es la Entidad Contratante en la persona de la Máxima Autoridad Ejecutiva de la institución.

1.13 Atribuciones

Son atribuciones de la Entidad Contratante, sin carácter limitativo, las siguientes:

a) Definir la Unidad Administrativa que tendrá la responsabilidad técnica de la gestión.
b) Nombrar a los Peritos.
c) Determinar funciones y responsabilidades por unidad partícipe y por funcionario vinculado al proceso.
d) Cancelar, declarar desierta o nula, total o parcialmente el Procedimiento de Excepción de Proveedor Único, por las causas que considere pertinentes. En consecuencia, podrá efectuar otras Licitaciones en los términos y condiciones que determine.

1.14 Órgano Responsable del Proceso

El Órgano responsable del proceso de Excepción de Proveedor Único es el Comité de Compras y Contrataciones. El Comité de Compras y Contrataciones está integrado por cinco (05) miembros:

- El funcionario de mayor jerarquía de la institución, o quien este designe, quien lo presidirá;
- El Director Administrativo Financiero de la entidad, o su delegado;
- El Consultor Jurídico de la entidad, quien actuará en calidad de Asesor Legal;
- El Responsable del Área de Planificación y Desarrollo o su equivalente;
- El Responsable de la Oficina de Libre Acceso a la Información.

1.15 Exención de Responsabilidades

El Comité de Compras y Contrataciones no estará obligado a declarar habilitado y/o Adjudicatario a ningún Oferente/Proponente que haya presentado sus Credenciales y/u Ofertas, si las mismas no demuestran que cumplen con los requisitos establecidos en el presente Pliego de Condiciones Específicas.

1.16 Prácticas Corruptas o Fraudulentas

Las prácticas corruptas o fraudulentas comprendidas en el Código Penal o en la Convención Interamericana contra la Corrupción, o cualquier acuerdo entre proponentes o con terceros, que establecieren prácticas restrictivas a la libre competencia, serán causales determinantes del rechazo de la propuesta en cualquier estado del procedimiento de selección, o de la rescisión del Contrato, si éste ya se hubiere celebrado. A los efectos anteriores se entenderá por:

a) **"Práctica Corrupta",** al ofrecimiento, suministro, aceptación o solicitud de cualquier cosa de valor con el fin de influir en la actuación de un funcionario público u obtener una ventaja indebida con respecto al proceso de contratación o a la ejecución del Contrato, y,

b) **"Práctica Fraudulenta",** es cualquier acto u omisión incluyendo una tergiversación de los hechos con el fin de influir en un proceso de contratación o en la ejecución de un Contrato de obra pública en perjuicio del contratante; la expresión comprende las prácticas colusorias entre los licitantes (con anterioridad o posterioridad a la presentación de las ofertas) con el fin de establecer precios de oferta a niveles artificiales y no competitivos y privar al contratante de las ventajas de la competencia libre y abierta, coercitivas y obstructiva.

1.17 De los Oferentes/ Proponentes Hábiles e Inhábiles

Toda persona natural o jurídica, nacional o extranjera que haya adquirido el Pliego de Condiciones, tendrá derecho a participar en el presente Procedimiento de Excepción de Proveedor Único, siempre y cuando reúna las condiciones exigidas y no se encuentre afectada por el régimen de prohibiciones establecido en el presente Pliego de Condiciones.

1.18 Prohibición a Contratar

No podrán participar como Oferentes/Proponentes, en forma directa o indirecta, las personas físicas o sociedades comerciales que se relacionan a continuación:

1) El Presidente y Vicepresidente de la República; los Secretarios y Subsecretarios de Estado; los Senadores y Diputados del Congreso de la República; los Magistrados de la Suprema Corte de Justicia, de los demás tribunales del orden judicial, de la Cámara de Cuentas y de la Junta Central Electoral; los Síndicos y

   Regidores de los Ayuntamientos de los Municipios y del Distrito Nacional; el Contralor General de la República y el Sub-contralor; el Director de Presupuesto y Subdirector; el Director Nacional de Planificación y el Subdirector; el Procurador General de la República y los demás miembros del Ministerio Público; el Tesorero Nacional y el Subtesorero y demás funcionarios de primer y segundo nivel de jerarquía de las instituciones incluidas bajo el ámbito de aplicación de la Ley No. 340-06;

2) Los jefes y subjefes de Estado Mayor de las Fuerzas Armadas, así como el jefe y subjefes de la Policía Nacional;

3) Los funcionarios públicos con injerencia o poder de decisión en cualquier etapa del procedimiento de contratación administrativa;

4) Todo personal de la entidad contratante;

5) Los parientes por consanguinidad hasta el tercer grado o por afinidad hasta el segundo grado, inclusive, de los funcionarios relacionados con la contratación cubiertos por la prohibición, así como los cónyuges, las parejas en unión libre, las personas vinculadas con análoga relación de convivencia afectiva o con las que hayan procreado hijos, y descendientes de estas personas;

6) Las personas jurídicas en las cuales las personas naturales a las que se refieren los Numerales 1 al 4 tengan una participación superior al diez por ciento (10%) del capital social, dentro de los seis meses anteriores a la fecha de la convocatoria;

7) Las personas físicas o jurídicas que hayan intervenido como asesoras en cualquier etapa del procedimiento de contratación o hayan participado en la elaboración de las especificaciones técnicas o los diseños respectivos, salvo en el caso de los contratos de supervisión;

8) Las personas físicas o jurídicas que hayan sido condenadas mediante sentencia que haya adquirido la autoridad de la cosa irrevocablemente juzgada por delitos de falsedad o contra la propiedad, o por delitos de cohecho, malversación de fondos públicos, tráfico de influencia, prevaricación, revelación de secretos, uso de información privilegiada o delitos contra las finanzas públicas, hasta que haya transcurrido un lapso igual al doble de la condena. Si la condena fuera por delito contra la administración pública, la prohibición para contratar con el Estado será perpetua;

9) Las empresas cuyos directivos hayan sido condenados por delitos contra la administración pública, delitos contra la fe pública o delitos comprendidos en las convenciones internacionales de las que el país sea signatario;

10) Las personas físicas o jurídicas que se encontraren inhabilitadas en virtud de cualquier ordenamiento jurídico;

11) Las personas que suministraren informaciones falsas o que participen en actividades ilegales o fraudulentas relacionadas con la contratación;

12) Las personas naturales o jurídicas que se encuentren sancionadas administrativamente con inhabilitación temporal o permanente para contratar con entidades del sector público, de acuerdo a lo dispuesto por la presente ley y sus reglamentos;

13) Las personas naturales o jurídicas que no estén al día en el cumplimiento de sus obligaciones tributarias o de la seguridad social, de acuerdo con lo que establezcan las normativas vigentes;

PARRAFO I: Para los funcionarios contemplados en los Numerales 1 y 2, la prohibición se extenderá hasta **seis (6) meses** después de la salida del cargo.

PARRAFO II: Para las personas incluidas en los Numerales 5 y 6 relacionadas con el personal referido en el Numeral 3, la prohibición será de aplicación en el ámbito de la institución en que estos últimos prestan servicio.

En adición a las disposiciones del Artículo 14 de la Ley No. 340-06 con sus modificaciones NO podrán contratar con el Estado dominicano los proveedores que no hayan actualizado sus datos en el Registro de Proveedores del Estado.

1.19 Demostración de Capacidad para Contratar

Los Oferentes/Proponentes deben demostrar que:

1) Poseen las calificaciones profesionales y técnicas que aseguren su competencia, los recursos financieros, el equipo y demás medios físicos, la fiabilidad, la experiencia y el personal necesario para ejecutar el contrato.
2) No están embargados, en estado de quiebra o en proceso de liquidación; sus negocios no han sido puestos bajo administración judicial, y sus actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en su contra por cualquiera de los motivos precedentes;

3) Han cumplido con sus obligaciones tributarias y de seguridad social;

4) Han cumplido con las demás condiciones de participación, establecidas de antemano en los avisos y el presente Pliego de Condiciones;

5) Se encuentran legalmente domiciliados y establecidos en el país, cuando se trate de licitaciones públicas nacionales;

6) Que los fines sociales sean compatibles con el objeto contractual;

1.20 Representante Legal

Todos los documentos que presente el Oferente/Proponente dentro del presente Procedimiento de Excepción de Proveedor Único deberán estar firmados por él, o su Representante Legal, debidamente facultado al efecto.

1.21 Subsanaciones

A los fines del presente Procedimiento de Excepción de Proveedor Único se considera que una Oferta se ajusta sustancialmente a los Pliegos de Condiciones, cuando concuerda con todos los términos y especificaciones de dichos documentos, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los oferentes es siempre subsanable.

La determinación de la Entidad Contratante de que una Oferta se ajusta sustancialmente a los documentos del Procedimiento de Excepción de Proveedor Único se basará en el contenido de la propia Oferta, sin que tenga que recurrir a pruebas externas.

Siempre que se trate de errores u omisiones de naturaleza subsanable entendiendo por éstos, generalmente, aquellas cuestiones que no afecten el principio de que las Ofertas deben ajustarse sustancialmente a los Pliegos de Condiciones, la Entidad Contratante podrá solicitar que, en un plazo breve, El Oferente/Proponente suministre la información faltante.

Cuando proceda la posibilidad de subsanar errores u omisiones se interpretará en todos los casos bajo el entendido de que la Entidad Contratante tenga la posibilidad de contar con la mayor cantidad

de ofertas validas posibles y de evitar que, por cuestiones formales intrascendentes, se vea privada de optar por ofertas serias y convenientes desde el punto de vista del precio y la calidad.

No se podrá considerar error u omisión subsanable, cualquier corrección que altere la sustancia de una oferta para que se la mejore.

La Entidad Contratante rechazará toda Oferta que no se ajuste sustancialmente al Pliego de Condiciones Específica. No se admitirán correcciones posteriores que permitan que cualquier Oferta, que inicialmente no se ajustaba a dicho Pliego, posteriormente se ajuste al mismo.

1.22 Rectificaciones Aritméticas

Para fines de subsanaciones, los errores aritméticos serán corregidos de la siguiente manera:

a) Si existiere una discrepancia entre una cantidad parcial y la cantidad total obtenida multiplicando las cantidades parciales, prevalecerá la cantidad parcial y el total será corregido.

b) Si la discrepancia resulta de un error de suma o resta, se procederá de igual manera; esto es, prevaleciendo las cantidades parciales y corrigiendo los totales.

c) Si existiere una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras.

Si el Oferente no acepta la corrección de los errores, su Oferta será rechazada.

1.23 Garantías

Los importes correspondientes a las garantías deberán hacerse en la misma moneda utilizada para la presentación de la Oferta. Cualquier garantía presentada en una moneda diferente a la presentada en la Oferta será descalificada sin más trámite.

Los Oferentes/Proponentes deberán presentar las siguientes garantías:

1.23.1 Garantía de la Seriedad de la Oferta

Correspondiente al uno por ciento (1%) del monto total de la Oferta.

PÁRRAFO I. La Garantía de Seriedad de la Oferta será de cumplimiento obligatorio y vendrá incluida dentro de la Oferta Económica. La omisión en la presentación de la Oferta de la Garantía de Seriedad de Oferta o cuando la misma fuera insuficiente, conllevará la desestimación de la Oferta sin más trámite.

1.23.2 Garantía de Fiel Cumplimiento de Contrato

Los Adjudicatarios cuyos Contratos excedan el equivalente en Pesos Dominicanos de **Diez Mil Dólares de los Estados Unidos de Norteamérica con 00/100 (US$10.000,00)**, están obligados a

constituir una Garantía Bancaria o Pólizas de Fianzas de compañías aseguradoras de reconocida solvencia en la República Dominicana, con las condiciones de ser incondicionales, irrevocables y renovables, en el plazo de **Cinco (5) días hábiles**, contados a partir de la Notificación de la Adjudicación, por el importe del **CUATRO POR CIENTO (4%)** del monto total del Contrato a intervenir, a disposición de la Entidad Contratante, cualquiera que haya sido el procedimiento y la forma de Adjudicación del Contrato. En el caso de que el adjudicatario sea una Micro, Pequeña y Mediana empresa (MIPYME) el importe de la garantía será de un **UNO POR CIENTO (1%).** La Garantía de Fiel Cumplimiento de Contrato debe ser emitida por una entidad bancaria de reconocida solvencia en la República Dominicana.

La no comparecencia del Oferente Adjudicatario a constituir la Garantía de Fiel Cumplimiento de Contrato, se entenderá que renuncia a la Adjudicación y se procederá a la ejecución de la Garantía de Seriedad de la Oferta.

Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, la Entidad Contratante, como Órgano de Ejecución del Contrato, notificará la Adjudicación de los renglones correspondientes al Oferente que hubiera obtenido la siguiente posición en el proceso de Adjudicación, conforme al Reporte de Lugares Ocupados. El nuevo Oferente Adjudicatario depositará la Garantía y suscribirá el Contrato de acuerdo al plazo que le será otorgado por la Entidad Contratante**,** mediante comunicación formal.

1.24 Devolución de las Garantías

a) **Garantía de la Seriedad de la Oferta:** Tanto al Adjudicatario como a los demás oferentes participantes una vez integrada la garantía de fiel cumplimiento de contrato.

b) **Garantía de Fiel Cumplimiento de Contrato:** Una vez cumplido el contrato a satisfacción de la Entidad Contratante, cuando no quede pendiente la aplicación de multa o penalidad alguna.

1.25 Consultas

Los interesados podrán solicitar a la Entidad Contratante aclaraciones acerca del Pliego de Condiciones Específicas, hasta la fecha que coincida con el **CINCUENTA POR CIENTO (50%)** del plazo para la presentación de las Ofertas. Las consultas las formularán los Oferentes por escrito, sus representantes legales, o quien éstos identifiquen para el efecto. La Unidad Operativa de Compras y Contrataciones, dentro del plazo previsto, se encargará de obtener las respuestas conforme a la naturaleza de la misma.

Las Consultas se remitirán al Comité de Compras y Contrataciones, dirigidas a:

COMITÉ DE COMPRAS Y CONTRATACIONES
Programa Administración Financiera Integrada (PAFI) del Ministerio de Hacienda
Referencia: **PAFI-CCC-PEPU-2018-0010**
Dirección: **Ave. México No. 45, Gazcue**
Teléfonos: **809-687-5131 ext. 2436**

Correo electrónico: yefernandez@hacienda.gov.do

1.26 Circulares

El Comité de Compras y Contrataciones podrá emitir Circulares de oficio o para dar respuesta a las Consultas planteadas por los Oferentes/Proponentes con relación al contenido del presente Pliego de Condiciones, formularios, otras Circulares o anexos. Las Circulares se harán de conocimiento de todos los Oferentes/Proponentes. Dichas circulares deberán ser emitidas solo con las preguntas y las respuestas, sin identificar quien consultó, en un plazo no más allá de la fecha que signifique el **SETENTA Y CINCO POR CIENTO (75%)** del plazo previsto para la presentación de las Ofertas y deberán ser notificadas a todos los Oferentes que hayan adquirido el Pliego de Condiciones Específicas y publicadas en el portal institucional y en el administrado por el Órgano Rector.

1.27 Enmiendas

De considerarlo necesario, por iniciativa propia o como consecuencia de una Consulta, el Comité de Compras y Contrataciones podrá modificar, mediante Enmiendas, el Pliego de Condiciones Específicas, formularios, otras Enmiendas o anexos. Las Enmiendas se harán de conocimiento de todos los Oferentes/Proponentes y se publicarán en el portal institucional y en el administrado por el Órgano Rector.

Tanto las Enmiendas como las Circulares emitidas por el Comité de Compras y Contrataciones pasarán a constituir parte integral del presente Pliego de Condiciones y en consecuencia, serán de cumplimiento obligatorio para todos los Oferentes/Proponentes.

1.28 Reclamos, Impugnaciones y Controversias

En los casos en que los Oferentes/Proponentes no estén conformes con la Resolución de Adjudicación, tendrán derecho a recurrir dicha Adjudicación. El recurso contra el acto de Adjudicación deberá formalizarse por escrito y seguirá los siguientes pasos:

1. El recurrente presentará la impugnación ante la Entidad Contratante en un plazo no mayor de diez (10) días hábiles a partir de la fecha del hecho impugnado o de la fecha en que razonablemente el recurrente debió haber conocido el hecho. La Entidad pondrá a disposición del recurrente los documentos relevantes correspondientes a la actuación en cuestión, con la excepción de aquellas informaciones declaradas como confidenciales por otros Oferentes o Adjudicatarios, salvo que medie su consentimiento.

2. En los casos de impugnación de Adjudicaciones, para fundamentar el recurso, el mismo se regirá por las reglas de impugnación establecidas en los Pliegos de Condiciones Específicas.

3. Cada una de las partes deberá acompañar sus escritos de los documentos que hará valer en apoyo de sus pretensiones. Toda entidad que conozca de un recurso deberá analizar toda la documentación depositada o producida por la Entidad Contratante.

4. La entidad notificará la interposición del recurso a los terceros involucrados, dentro de un plazo de **dos (2) días hábiles**.

5. Los terceros estarán obligados a contestar sobre el recurso dentro de **cinco (5) días calendario**, a partir de la recepción de notificación del recurso, de lo contrario quedarán excluidos de los debates.

6. La entidad estará obligada a resolver el conflicto, mediante resolución motivada, en un plazo no mayor de **quince (15) días calendario**, a partir de la contestación del recurso o del vencimiento del plazo para hacerlo.

7. El Órgano Rector podrá tomar medidas precautorias oportunas, mientras se encuentre pendiente la resolución de una impugnación para preservar la oportunidad de corregir un incumplimiento potencial de esta ley y sus reglamentos, incluyendo la suspensión de la adjudicación o la ejecución de un Contrato que ya ha sido Adjudicado.

8. Las resoluciones que dicten las Entidades Contratantes podrán ser apeladas, cumpliendo el mismo procedimiento y con los mismos plazos, ante el Órgano Rector, dando por concluida la vía administrativa.

Párrafo I.- En caso de que un Oferente/Proponente iniciare un procedimiento de apelación, la Entidad Contratante deberá poner a disposición del Órgano Rector copia fiel del expediente completo.

Párrafo II.- La presentación de una impugnación de parte de un Oferente o Proveedor, no perjudicará la participación de éste en Licitaciones en curso o futuras, siempre que la misma no esté basada en hechos falsos.

Las controversias no resueltas por los procedimientos indicados en el artículo anterior serán sometidas al Tribunal Superior Administrativo, o por decisión de las partes, a arbitraje.

La información suministrada al Organismo Contratante en el proceso de Excepción de Proveedor Único, o en el proceso de impugnación de la Resolución Administrativa, que sea declarada como confidencial por el Oferente, no podrá ser divulgada si dicha información pudiese perjudicar los intereses comerciales legítimos de quien la aporte o pudiese perjudicar la competencia leal entre los Proveedores.

1.29 Comisión de Veeduría

Las Veedurías son el mecanismo de control social, que de manera más concreta, acerca a la comunidad al ejercicio y desempeño de la gestión pública y la función administrativa.

Sección II
Datos del Procedimiento de Excepción de Proveedor Único (DDPEPU)

2.1 Objeto de la Procedimiento de Excepción de Proveedor Único

Constituye el objeto de la presente convocatoria la **Ampliación de las Soluciones de Web Application Firewall, Application Delivery, Balanceo de Aplicaciones y Protección de DDOS; Gateways de Manejo y Control de Seguridad Integrada y Software de Seguridad para la Infraestructura de Virtualización del Ministerio de Hacienda,** de acuerdo con las condiciones fijadas en el presente Pliego de Condiciones Específicas.

2.2 Procedimiento de Selección

Este Procedimiento de Selección será de Etapa Única

2.3 Fuente de Recursos

El Programa de Administración Financiera Integrada (PAFI) del Ministerio de Hacienda, de conformidad con el Artículo 32 del Reglamento No. 543-12 sobre Compras y Contrataciones Públicas de Bienes, Servicios y Obras, ha tomado las medidas previsoras necesarias a los fines de garantizar la apropiación de fondos correspondiente, dentro de los Presupuestos de los años **2018, 2019, 2020 y 2021** que sustentarán el pago de todos los servicios contratados mediante la presente Licitación. Las partidas de fondos para liquidar las entregas programadas serán debidamente especializadas para tales fines, a efecto de que las condiciones contractuales no sufran ningún tipo de variación durante el tiempo de ejecución del mismo.

2.4 Condiciones de Pago

La Entidad Contratante establece de siguiente modalidad de pago:

(i) **Anticipo:** El veinte por ciento (20%) del precio del Contrato, se pagará dentro de los treinta (30) días calendario siguientes a la entrega de la garantía de buen del anticipo; *

(ii) **Al colocar la orden en fabrica de los bienes y servicios conexos::** El cincuenta por ciento (50%) del precio del Contrato, se pagará dentro de los treinta (30) días calendario siguientes de que el proveedor concluya de forma exitosa la "instalación de la aplicación".

(iii) **Al entregar los bienes y servicios conexos":** El veinte por ciento (20%) del precio del Contrato, se pagará dentro de los treinta (30) días calendario siguientes de:

(iv) **Puesta en marcha y funcionamiento de los bienes y servicios conexos":** El diez por ciento (10%) del precio del Contrato, se pagará dentro de los treinta (30) días calendario siguientes de:

*En caso de requerirse la garantía de buen uso de anticipo, deberá ser constituida por el equivalente al monto que reciba el adjudicatario, conforme a lo establecido en el artículo 112 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, Reglamento de Aplicación de la Ley No. 340-06 y sus modificaciones.

2.5 Cronograma del Procedimiento de Excepción de Proveedor Único[2]

ACTIVIDADES	PERÍODO DE EJECUCIÓN
1. Publicación llamado a participar en la licitación	**Jueves 27 de septiembre del año 2018**
2. Período para realizar consultas por parte de los interesados	50% del plazo para presentar Ofertas **del año 2018**
3. Plazo para emitir respuesta por parte del Comité de Compras y Contrataciones	No más allá de la fecha que signifique el 75% del plazo para presentar Ofertas. **del año 2018**
4. **Recepción de Propuestas: "Sobre A" y "Sobre B" y apertura de "Sobre A" Propuestas Técnicas** y **"Sobre B" Propuestas Económicas.**.	**Lunes 01 de Octubre del año 2018 Desde las 8:00AM hasta las 10:00AM en la Dirección Jurídica.** **Apertura: 11:30AM**
5. Verificación, Validación y Evaluación contenido de las Propuestas Técnicas "Sobre A" y Homologación de Muestras, si procede.	Plazo razonable conforme al objeto de la contratación **Miércoles 03 de Octubre del año 2018**
6. Notificación de errores u omisiones de naturaleza subsanables.	Plazo razonable conforme al objeto de la contratación **Jueves 04 de Octubre del año 2018**
7. Periodo de subsanación de ofertas	Plazo razonable conforme al objeto de la Contratación **Lunes 08 de Octubre del año 2018**
8. Período de Ponderación de Subsanaciones	Plazo razonable conforme al objeto de la contratación **Miércoles 10 de Octubre del año 2018**
9. Adjudicación	**Jueves 11 de Octubre del año 2018**
10. Notificación y Publicación de Adjudicación	5 días hábiles a partir del Acto Administrativo de Adjudicación
11. Plazo para la constitución de la Garantía Bancaria de Fiel Cumplimiento de Contrato	Dentro de los siguientes 05 días hábiles, contados a partir de la Notificación de Adjudicación

[2] **Nota:** Incluir en el cronograma una actividad de reunión técnica o aclaratoria, si procede.

12. Suscripción del Contrato	No mayor a 20 días hábiles contados a partir de la Notificación de Adjudicación
13. Publicación de los Contratos en el portal institución y en el portal administrado por el Órgano Rector.	Inmediatamente después de suscritos por las partes

2.6 Disponibilidad y Adquisición del Pliego de Condiciones

El Pliego de Condiciones estará disponible, en la fecha indicada en el Cronograma de la Licitación, en la página Web de la institución http://www.hacienda.gov.do/ y en el portal administrado por el Órgano Rector**,** www.comprasdominicana.gov.do, para todos los interesados.

El Oferente que adquiera el Pliego de Condiciones a través de la página Web de la institución, **http://www.hacienda.gov.do/** o del portal administrado por el Órgano Rector, www.comprasdominicana.gov.do, deberá enviar un correo electrónico a yefernandez@hacienda.gov.do, o en su defecto, notificar al **Ministerio de Hacienda** sobre la adquisición del mismo, a los fines de que la Entidad Contratante tome conocimiento de su interés en participar.

2.7 Conocimiento y Aceptación del Pliego de Condiciones

El sólo hecho de un Oferente/Proponente participar en el Procedimiento de Excepción de Proveedor Único implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos y su Representante Legal, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente Pliego de Condiciones, el cual tienen carácter jurídicamente obligatorio y vinculante.

2.8 Descripción de Bienes y Servicios Conexos

La entidad contratante deberá tener pendiente que al momento de confeccionar el Pliego de Condiciones Específicas, deberá distribuirse la cantidad total de cada producto en diferentes renglones, en los casos en que una misma convocatoria abarque un número importante de unidades, con el objeto de estimular la participación de las micro, pequeñas y medianas empresas.

Ministerio de Hacienda de la República Dominicana			
Términos de Referencia Técnicos			
Ampliación de las Soluciones de Web Application Firewall, Application Delivery, Balanceo de Aplicaciones y Protección de DDOS; Gateways de Manejo y Control de Seguridad Integrada y Software de Seguridad para la Infraestructura de Virtualización del Ministerio de Hacienda.			
NO Partida	**Cantidad**	***Descripción***	**Especificaciones Técnicas**
1.000		***Expansión de la Solución de Gateways de Manejo y Control de Seguridad Integrada redundantes para Firewall.***	
1.001	***1***	***Expansión de la Solución de***	Los Gateways de Manejo y Control de Seguridad

		Gateways de Manejo y Control de Seguridad Integrada redundantes para Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación y Extracción de Amenazas, VPNs Ipsec, Data Loss Prevention e integración con la solución de Sandboxing. La solución actual está basada en equipos Checkpoint.	Integrada redundantes deben estar configurados en un esquema de alta disponibilidad con fuentes de poder y abanicos de enfriamiento redundantes y deben cumplir con un mínimo de las siguientes configuraciones y ser capaces de manejar los siguientes aspectos de seguridad cada uno:
1.002			115 Gbps de Throughput de Firewall 20 Gbps de Throughput de IPS 20 Gbps de Throughput de Next Generation Firewall 15 Gbps de Throughput de Threat Prevention Discos Duros SSD redundantes con un mínimo de 450 GB cada uno Cinco (5) slots de expansión para tarjetas de interfases de redes Puerto de Consola, Puerto para Gerencia Lights Out, Puerto de Gerencia 10/100/1000 RJ45 10 puertos de Conexiones a 10/100/1000 RJ45 10 puertos de Conexiones a 10 Gbps SFP+ con los Módulos de Conexión de Fibra Óptica Multimodo 2 puertos de Conexión a 40 Gbps QSFP+ con los Módulos de Conexión de Fibra Óptica Multimodo
1.003			Debe ser capaz de soportar, estar configurada y licenciada para manejar un mínimo de 10 firewalls virtuales. Debe soportar control de acceso para por lo menos 150 servicios y/o protocolos predefinidos
1.004			Debe permitir definir reglas de seguridad que puedan ser enforzadas dentro de intervalos de tiempo configurados con tiempo y fecha de expiración. Debe manejar estadísticas de conteo de la utilización de cada una de las reglas de seguridad y enviar las mismas a la aplicación de gerencia de la aplicación.
1.005			Debe soportar métodos de autenticación basados en clientes, usuarios y sesiones.
1.006			La comunicación entre los servidores de gerencia y los Gateways de Seguridad deben ser encriptados y autenticados con Certificados PKI
1.007			Debe soportar DCHP, server y relay. Debe incluir una base de datos de usuarios local que permita la autenticación y autorización sin necesidad de ningún dispositivo externo.

1.008			Deben soportarse los siguientes esquemas de autenticación de usuarios: Tokens (SecureID), TACACS, RADIUS y Certificados Digitales
1.009			Debe soportar y estar configurada en Alta Disponibilidad en los Gateways con balanceo de carga y sincronización de estado. Debe ser capaz de trabajar en modo Bridge/Transparente y soportar HTTP y proxy PTTPS
1.010			Debe soportar la configuración de gateways en stacks dobles o con un interfase de unión o como una sub-interfase de un interfase de unión.
1.011			Debe soportar tráfico IPv6 en los módulos de IPS, APP, Firewall, Identity Awareness, filtrado URL, Antivirus y Anti BOT. Debe soportar NAT 6 a 4, o túneles 6 a 4. Debe soportar integración AD usando tráfico IPv6
1.012			Debe soportar seguimiento y logs que muestren el tráfico IPv6. Debe soportar la habilidad de mostrar tablas de ruteo IPv6.
1.013			La solución debe soportar los siguientes RFCs IPv6:
1.014			RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
1.015			RFC 2460 IPv6 Basic specification
1.016			RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
1.017			RFC 3596 DNS Extensions to support IPv6
1.018			RFC 4007 IPv6 Scoped Address Architecture
1.019			RFC 4193 Unique Local IPv6 Unicast Addresses
1.020			RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.
1.021			RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)
1.022			RFC 4443 ICMPv6
1.023			RFC 4861 Neighbor Discovery
1.024			RFC 4862 IPv6 Stateless Address Auto-configuration
1.025			La solución de IPS debe mínimamente permitir los mecanismos de detección basados en exploit signatures, anomalías de protocolos, y detección por el control y el comportamiento de las aplicaciones
1.026			La solución debe pertenecer al cuadrante de líderes del Cuadrante Mágico de Gartner para las soluciones de Firewall e IPS
1.027			Las soluciones de IPS y de Firewall deben estar integradas en una única plataforma
1.028			La administración de la solución de IPS debe permitir que se configure la inspección para proteger solamente los hosts internos. El IPS debe tener las opciones de crear perfiles para protección de clientes, servidores o

			una combinación de ambos.
1.029			La solución de IPS debe proveer pre configurada por lo menos dos perfiles y/o políticas que puedan ser usadas de forma inmediata
1.030			Los IPS deben tener un mecanismo basado en fail-open que pueda ser configurado en base a límites del uso de la memoria y los CPUs de los Gateways
1.031			Los IPS deben ser capaces de activar o manejar mecanismos automáticos de nuevas firmas desde las actualizaciones. Deben soportar excepciones de redes basadas en la fuente, el destino, el servicio o una combinación de las tres anteriores.
1.032			Los IPS deben incluir una modalidad de Troubleshooting que permita al perfil en uso que solo detecte sin modificar las protecciones individuales
1.033			La solución de IPS debe tener un mecanismo centralizado de correlación y reporte de eventos. El administrador debe ser capaz de activar automáticamente nuevas protecciones basadas en parámetros configurables tales como impacto de rendimiento, severidad de las amenazas, niveles de confianza, protecciones a los clientes y protecciones a los servidores.
1.034			La solución de IPS debe se capaz de detectar y prevenir las amenazas siguientes: Mal uso de protocolos, comunicaciones de Malware, intentos de uso de túneles, y tipos de ataques genéricos sin firmas predeterminadas. Para cada protección, la solución debe incluir tipos de protección para clientes y servidores, severidad de las amenazas, impacto en el rendimiento, niveles de confianza y referencias de la industria.
1.035			Los IPS deben ser capaces de recolectar capturas de paquetes para protecciones específicas. Deben ser capaces de detectar y bloquear ataques a niveles de red y de aplicaciones, protegiendo un mínimo de los siguientes servicios: email, DNS, FTP, y Servicios de Windows (Microsoft Networking). La solución debe ser líder protegiendo las vulnerabilidades de Microsoft
1.036			Los IPS y los controles de aplicaciones deben incluir la habilidad para detectar y bloquear aplicaciones P2P y evasivas. El administrador debe ser capaz de definir las redes y los hosts a ser excluidos de la inspección de los IPS

1.037			Los IPS deben proteger del Envenenamiento del Cache del DNS y prevenir a los usuarios de accesar las direcciones de dominios bloqueados. Debe proveer protección a los protocolos de VOIP
1.038			Los IPS y los controles de aplicaciones deben detectar y bloquear las aplicaciones de control remoto, incluyendo aquellas que son capaces de manejar túneles sobre tráfico HTTP. Deben incluir protección a protocolos SCADA y tener un mecanismo para convertir firmas SNORT.
1.039			La solución debe poder enforzar los protocolos de Citrix. Debe permitir al administrador a bloquear fácilmente el tráfico outbound o inbound basado en los Paises, sin necesidad de manejar manualmente rangos de direcciones IP correspondientes a esos países.
1.040			La solución de Adquisición de la Identidad del Usuario debe ser capaz de adquirir la identidad del usuario solicitando la misma al Microsoft Active Directory basada en los eventos de seguridad
1.041			Debe ofrecer un método de Autenticación de Identidad de Usuario basado en browser para los usuarios o activos que no pertenecen a dominio. Debe tener un agente de cliente dedicado que pueda ser instalado por políticas en las computadoras de los usuarios que puedan adquirir y reportar las identidades a los Gateways de Seguridad
1.042			Debe soportar ambientes de terminal servers. Debe integrarse de forma nativa con servicios de directorios, IF-MAP y RADIUS
1.043			El impacto de estos servicios debe ser menor al 3% en los controladores de dominio. La solución debe soportar terminales y servidores Citrix
1.044			La solución debe permitir la identificación a través de un proxy. Debe ser capaz de adquirir la identidad del usuario del Microsoft Active Directory sin necesidad de instalar ningún agente en los controladores de dominio.
1.045			Debe soportar autenticación transparente de Kerberos mediante un sign on único. Debe soportar el uso de grupos anidados de LDAP. Debe ser capaz de compartir y propagar identidades de usuarios entre múltiples gateways de seguridad y crear roles de identidad que puedan ser usados a través de todas las aplicaciones de seguridad
1.046			La base de datos de la Solución para Control de Aplicaciones y Filtrado de URL debe contener más de 6000 aplicaciones conocidas. Debe tener una categorización de URLs que contenga mas de 200 millones de URLs y que cubra más del 85% del millón de

			sitios topes de Alexa
1.047			La solución debe ser capaz de crear reglas de filtrado con múltiples categorías. Debe ser capaz de crear filtros para un único site.
1.048			Debe tener granularidad de usuarios y grupos para las reglas de seguridad.
1.049			Los Caches locales de los Gateways de Seguridad deben ser capaces de ofrecer respuestas al 99% de los requerimientos de categorizaciones de los URLs dentro de las primeras 4 semanas luego de la entrada en producción de los mismos
1.050			Debe poseer un interfase fácil, que permita búsquedas para las aplicaciones y los URLs. La solución debe ser capaz de categorizar las aplicaciones y los URLs en base a Factores de Riesgo. El control de las aplicaciones y las políticas de seguridad de los URLF debe ser capaz de ser definido en base a las identidades de los usuarios.
1.051			El control de las aplicaciones y la base de datos de URLF debe ser capaz de ser actualizados mediante servicios en la nube. Debe poder manejar reglas unificadas para el control de aplicaciones y de URLF
1.052			La solución debe proveer mecanismos para informar o preguntar a los usuarios en tiempo real para educarlos o confirmar acciones basadas en las políticas de seguridad.
1.053			La solución debe ser capaz de proveer un mecanismo para limitar el uso de aplicaciones basado en el consumo de ancho de banda de las mismas. Debe permitir excepciones de redes basadas en objetos de redes definidos.
1.054			La Solución debe proveer opciones de modificar la Notificación de Bloqueo y re direccionar al usuario a una página de remediación. Debe incluir mecanismos de Listas Blancas y Negras, y permitir al administrador negar o permitir acceso a URLs específicas independientemente de las categorías.
1.055			La solución debe tener mecanismos configurables de Bypass. Debe proveer un mecanismo de override para la categorización de la base de datos de URLS.
1.056			El control de las aplicaciones y las políticas de seguridad de los URLF deben reportar el conteo de usos de las reglas
1.057			La solución debe incluir las aplicaciones de Anti-BOT y Anti-Virus integradas en los Gateways de Seguridad.

1.058			La aplicación de Anti-BOT debe ser capaz de detectar y detener comportamientos anormales o sospechosos de la red. Debe utilizar un motor de detección de multi-niveles que incluya la reputación de las direcciones Ips, los URLs y las Direcciones de DNS y que detecte patrones de comunicaciones de BOTs. Las protecciones Anti-BOT deben ser capaces de realizar búsquedas de acciones de BOT.
1.059			La solución debe soportar la detección y prevención de virus tipo Cryptors y Ransomware y sus variantes mediante análisis dinámicos y/o estáticos. Debe ser capaz de proteger contra ataques tipo spear phishing.
1.060			Debe poseer capacidades de detección y prevención de C&C DNS hide outs. Debe ser capaz de determinar patrones de tráfico C&C, no solo en su destino de DNS
1.061			Debe ser capaz de realizar ingeniería de reversa para descubrir su DGA (Domain Name Generation). Debe poseer características para manejar traps de DNS para la prevención de amenazas y asistencia en el descubrimiento de hosts infectados que generan comunicaciones C&C. Debe tener capacidades de detección y prevención para proteger de ataques mediante túneles de DNS
1.062			Las políticas de Anti-BOT y Anti-Virus deben poder administrarse desde una consola central. Las aplicaciones de Anti-BOT y Anti-Virus deben tener un mecanismo centralizado de correlación y reportes de eventos.
1.063			La aplicación de Anti-Virus debe ser capaz de prevenir acceso a websites maliciosos e inspeccionar tráfico SSL encriptado. Debe ser capaz de detener archivos maliciosos de entrada. Debe poder escanear archivos almacenados.
1.064			Las soluciones de Anti-BOT y Anti-Virus deben recibir actualizaciones en tiempo real de servicios de reputación basados en la nube. Deben ser capaces de manejar políticas de configuración y enforzamiento granulares de manera centralizada.
1.065			El Anti-Virus debe soportar mas de 50 motores de Anti-Virus basados en la nube. Debe soportar escaneo de links dentro de los emails y escanear archivos que están pasando mediante el protocolo CIFS
1.066			La solución debe incluir la Inspección SSL tanto de tráfico entrante como saliente. Debe soportar la Inspección/Decriptamiento con rendimiento líder a través de todas las tecnologías de mitigación

1.067			Debe soportar Perfect Forward Secrecy (PFS, ECDHE conjuntos de cifrado), y AES-NI, AES-GCM para mejoras en el flujo
1.068			Deben incluirse funcionalidades para la emulación de amenazas y sandboxing integradas a la inspección de SSL.
1.069			La solución debe aprovechar la base de datos de filtrado de URLs para permitirle al administrador crear políticas de inspección de URLs granulares. Debe ser capaz de inspeccionar filtrado de URLs basado en HTTPS sin requerir decripción SSL
1.070			La solución debe ofrecer la funcionalidad de coordinación e integración con soluciones de Emulación de Amenazas (Sandboxing).
1.071			Debe proveer la habilidad de proteger contra ataques de malware y Zero-Day antes de que las protecciones de firmas estáticas hayan sido creadas. Deben proveer prevención en tiempo real de malware de Paciente-0 en Web Browsing y email
1.072			La Solución de Seguridad debe ser una arquitectura de prevención de amenazas completa y multinivel con mínimo de funcionalidades de: IPS, AV, AB, URLF, APP FW
1.073			La Solución de Seguridad debe soportar emulación de amenazas basada en Redes y Hosts. Debe ser capaz de soportar implementaciones basadas en sitio y en la nube. Se debe incluir en esta propuesta la integración con una solución basada en hosts locales instalados en las premisas de la institución
1.074			La solución debe soportar integración de terceros mediante APIs públicos. Debe soportar implementación en modo Inline, MTA (Mail Transfer Agent), inspect TLS y SSL. Debe soportar implementación en modo de puerto TAP/SPAN
1.075			La solución no debe requerir infraestructura separada para protección de email y protección de WEB.
1.076			Los dispositivos deben soportar instalación en Clusters de alta disponibilidad y deben estar configurados y ofertados en este esquema
1.077			La solución debe ser capaz de emular archivos almacenados ejecutables, documentos JAVA y FLASH, específicamente:
1.078			7z, cab,csv,doc, docm, docx,dot,dotm, exe, jar, pdf, potx,pps, ppsm, ppsx, ppt, pptm, pptx,rar, rtf, scr,swf,tar, xla,xls,xlsb, xlsm,xlsx,xlt,xltm,xltx,xlw,zip,pif,com,gz,bz2,tgz,apk,ipa,ISO,js,cpl,vbs,jse,vba,bve,wsf,wsh

1.079			La solución debe ser capaz de emular ejecutables, archivos almacenados, documentos, JAVA y Flash específicamente dentro de los siguientes protocolos:
1.080			HTTP,HTTPS,FTP,SMTP,CIFS(SMB), SMTP TLS
1.081			El motor de emulación debe soportar múltiples sistemas operativos tales como Windows 7,8,10 a 32/64 gbits incluyendo imágenes customizadas. La solución debe ofrecer el soporte de licencias prepopuladas de copias de imágenes Microsoft Windows y Office mediante un acuerdo con Microsoft
1.082			El motor de la solución debe detectar llamados a APIs, cambios en los archivos del sistema, los registros, las conexiones de redes y los procesos del sistema. Debe soportar análisis estático para Windows, mac OS-X, Linux o cualquier plataforma x86
1.083			El motor de emulación de la tecnología de Sandboxing debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing en la infraestructura de anti-malware
1.084			La solución debe ser capaz de realizar filtrado estático pre-emulación. La solución debe permitir la emulación de archivos de un tamaño mayor de 10Mb en todos los tipos soportados. Debe soportar motores de detección basados en aprendizaje automático de máquinas.
1.085			La solución debe detectar el ataque en el nivel de explotación, es decir, antes que el código Shell sea ejecutado y antes que el malware sea bajado/ejecutado. Debe ser capaz de detectar los ROP y otras técnicas de explotación tales como escalación de privilegios monitoreando el flujo del CPU
1.086			La solución debe ser capaz de soportar links de escaneo dentro de los emails para malwares desconocidos y de Día0. Debe ser capaz de escanear los URLS históricos almacenados los últimos X días y comprobar si los ratings han cambiado, por ejemplo, de rating limpio a malicioso.
1.087			El tiempo de emulación promedio para determinar un veredicto como benigno no debe tomar más de 1 minuto. El tiempo de emulación promedio para determinar un veredicto de un malware sospechoso como malware no debe tomar más de 3 minutos
1.088			La solución de emulación de amenazas debe permitir Restricciones Geográficas, las cuales permiten que las emulaciones sean restringidas a Países en específico.
1.089			La solución debe proveer la habilidad de incrementar la seguridad compartiendo automáticamente la información de nuevos ataques con otros Gateways

			utilizando la actualización de firmas entre otros
1.090			El motor de emulación debe exceder un 90% de captura en las pruebas de Virus Totales donde los pdf´s y exe´s son modificados con encabezados ¨no usados¨ para demostrar la capacidad de la solución para detectar malware nuevo y desconocido. La solución debe detectar tráfico C&C de acuerdo la reputación dinámica de los ip/url
1.091			La Solución debe ser capaz de emular y extraer archivos embebidos en documentos. Debe ser capaz de escanear documentos que contengan URLs
1.092			La solución debe monitorear las actividades sospechosas en:
1.093			Llamadas a APIs, Cambios en archivos del Sistema, Registro del Sistema, Conexiones de redes, Procesos del Sistema, Creación y borrado de archivos, Modificaciones de Archivos, Inyección de código al Kernel, Detección de intentos de escalamiento de privilegios, Modificaciones al Kernel (Cambios de memoria realizados por el código del Kernel, no el hecho de que se cargue un driver, esto esta cubierto por el elemento anterior), Comportamiento del código del Kernel, monitoreo de las actividades de código que no sea modalidad de usuario. Interacción física directa con el CPU, Detección de Bypass del Control de Acceso de Usuario.
1.094			La solución debe poseer capacidades de anti-evasión detectando la ejecución del Sandbox. Debe ser resiliente a casos donde el código shell o el malware puede no ejecutarse si detectan la existencia de un ambiente virtual (Hipervisor propietario). Debe ser resiliente a delays implementados en las etapas del código shell o el malware. Debe ser resiliente a casos donde el código shell o el malware solo se ejecute luego de un reinicio o apagado del end point.
1.095			La solución debe emular actividades de usuarios reales tales como clicks del ratón, uso del teclado, etc. Debe ser capaz de identificar íconos que son similares a documentos de aplicaciones populares. Debe proteger contra evasión dentro de archivos flash (swf)
1.096			La solución debe ofrecer la funcionalidad de poder ser manejada de forma centralizada. Luego de la detección de archivos maliciosos, se debe generar un reporte detallado para cada uno de los archivos maliciosos. El reporte detallado debe incluir capturas de pantallas, líneas de tiempo, las modificaciones o creaciones clave

			en el registry, la creación de archivos y/o procesos, y la actividad de red detectada
1.097			La solución debe eliminar las amenazas y remover el contenido explotable, incluyendo el contenido activo y los objetos embebidos. Debe ser capaz de reconstruir los archivos con los elementos seguros conocidos. Debe tener la capacidad de convertir los archivos reconstruidos a formato PDF. Debe mantener la flexibilidad de mantener el formato original del archivo y especificar el tipo de contenido que será removido.
1.098			La solución de seguridad de Anti-Spam y Email debe ser agnóstica al lenguaje y al contenido. Debe poseer clasificación y protección en tiempo real basados en la detección de brotes de spam que están basados en patrones y no en contenido. Debe incluir el bloqueo de IPs basados en reputación desde un servicio online para evitar falsos positivos
1.099			Debe incluir mecanismos de protección de Hora Cero para nuevos virus propagados a través de email y spam sin depender solamente en inspección de contenido o heurística
1.100			Para las funcionalidades de Ipsec VPNs debe soportar CA internos y externos de terceros. Debe soportar criptografía 3DES y AES-256 para IKE fase 1 y IIIKEv2 , Suite-B-GCM-128 y Suite B-GCM-256 para fase II.
1.101			Debe soportar por lo menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20. Debe soportar integridad de Data con md5, sha1SHA-256, SHA-384 y AES-XCBC
1.102			La solución debe soportar VPN sitio a sitio en las siguientes topologías: Full Mesh (all to all), Star (Oficinas remotas con sitio principal), Hub and Spoke (Sitio Remoto a través del Sitio Central con otro Sitio Remoto). Debe soportar la configuración de los VPNs mediante un GUI que permita la adición de objetos a las comunidades de VPNs mediante drag and drop.
1.103			Debe soportar SSL VPN clientless para acceso remoto. Deben soportar VPNs L2TP incluyendo los clientes para Iphones.

1.104			Debe permitir que el administrador aplique las reglas de seguridad para controlar el tráfico dentro de los VPNs. Debe soportar VPNs basados en dominios, y rutas usando protocolos de ruteo dinámico y VTIs. Debe incluir la habilidad de establecer VPNs dentro de gateways con IPs dinámicas públicas y compresión IP para VPNs cliente a sitio y sitio a sitio.
1.105			La aplicación de manejo de seguridad debe soportar cuentas de administradores basadas en roles, ejemplo, un rol solo para establecimiento de las políticas de firewall o un rol solo para visualización. Debe incluir canales de comunicación seguros basados en encripción de Certificados para todas las soluciones de diferentes fabricantes que pertenezcan a un dominio de gerencia.
1.106			La solución debe incluir una Autoridad de Certificados Interna, x509 CA que pueda generar Certificados a gateways y usuarios para permitir un mecanismo eficiente de autenticación en los VPNs. Debe incluir la capacidad de usar CA s externos que soporten estándares PKCS#12, CAPI o ENTRUST
1.107			Todas las aplicaciones de seguridad en este grupo deben ser capaces de ser manejadas desde una consola central. La solución de gerencia debe proveer un conteo de los hits a las reglas de seguridad en las políticas de seguridad. Debe incluir opciones de búsqueda que permitan investigar cual objeto de red contiene una dirección IP específica o una parte de ella.
1.108			Debe incluir la opción de segmentar la base de reglas utilizando etiquetas o títulos de secciones para mejor organización de las políticas. Debe proveer la opción de salvar la política completa o una parte específica de la misma. Debe poseer mecanismos de verificación de políticas de seguridad previo a la instalación de las mismas. Debe poseer mecanismos de control de revisión de las políticas de seguridad.
1.109			La solución debe proveer las opciones de añadir alta disponibilidad a la gerencia de seguridad, usando un servidor de gerencia standby que se sincroniza automáticamente con el servidor activo sin la necesidad de dispositivos externos de almacenamiento. Esta funcionalidad debe ser incluida en las propuestas de la licitación.
1.110			La solución de seguridad debe incluir un mapa comprensivo de todos los objetos de redes y sus conexiones que pueda ser exportado a Microsoft Visio o a un archivo de imágenes.

1.111			Debe incluir la habilidad de distribuir y aplicar de forma centralizada nuevas versiones de software a los diferentes gateways de seguridad. Debe incluir una herramienta de manejo de las licencias de los diferentes gateways de seguridad que debe ser controlada por la estación de gerencia. Debe tener la capacidad de manejo de multi dominios y soportar la funcionalidad de políticas de seguridad globales a través de los dominios.
1.112			El interfase gráfico de la herramienta de gerencia debe tener la habilidad de poder excluir direcciones IP de la definición de firmas de la solución de IPS. Debe tener la capacidad de excluir direcciones IP de los logs de IPS cuando se detectan como falsos positivos. Debe ser capaz de alcanzar las definiciones de firmas de IPS desde los logs de IPS.
1.113			El licitante debe proveer los detalles de sus mecanismos de actualización y de su habilidad para manejar ataques de día cero a través de todas las soluciones de prevención de amenazas incluyendo IPS, Control de Aplicaciones, Filtrado de URL, Anti BOT y anti Virus. Debe proveer los detalles de la categorización de los URLs bajo las circunstancias de que ese website haya sido comprometido y este distribuyendo malware
1.114			El mecanismo de logging central debe ser parte del sistema de administración, los administradores deben tener la capacidad de instalar servidores de almacenamiento de Logs adicionales.
1.115			La operación de logs debe proveer la opción de operar en el servidor de gerencia o en servidores dedicados. Debe ser capaz de operar en servidores X86 abiertos. Se debe entregar la lista de compatibilidad. La solución debe tener la habilidad de almacenar todos los logs para todas las reglas de seguridad. El buscador de logs debe tener la capacidad de realizar búsquedas indexadas.
1.116			La solución debe tener la capacidad de hacer logs a todas las aplicaciones integradas en esta solución, incluyendo IPS, Aplication Control, URL Filtering, Antivirus, AntiBOT, User Identity.
1.117			La solución debe incluir un mecanismo de captura automática de paquetes para los eventos de IPS de forma tal que se puedan realizar mejores análisis forénsicos. Debe proveer diferentes logs para regular las actividades de los usuarios y los relacionados a la gerencia.

1.118			La solución debe proveer para cada ocurrencia de un hit de reglas de seguridad las siguientes opciones: LOG, alerta, trap SNMP, email o la ejecución de un script definido por el usuario. Los LOGs debe tener un canal seguro de comunicaciones para la transferencia de los mismos para evitar escuchas, esta solución debe estar autenticada y encriptada. Los logs deben ser transferidos de manera segura entre el gateway, la gerencia, los servidores dedicados de LOGs y las consolas de visualización en las estaciones de los administradores
1.119			La solución debe incluir la opción de bloquear dinámicamente una conexión activa desde el interfase gráfico del LOG sin necesidad de modificar las bases de reglas. Debe ser capaz de exportar logs en formato de bases de datos. Debe soportar el cambio automático del archivo de LOGs basado en tiempos preestablecidos o en el tamaño de los archivos
1.120			Debe soportar el manejo de excepciones a los enforzamientos IPS desde el record de LOG. Debe ser capaz de asociar un nombre de usuario y un nombre de máquina a cada record de LOG.
1.121			La herramienta de manejo gráfica debe ser capaz de monitorear fácilmente el estatus de los gateways. Esta herramienta debe proveer información del sistema para cada gateway, incluyendo: uso de memoria, CPU, particiones de discos y espacio restante. Debe proveer el status de cada componente del gateway tales como firewall, vpn, clúster, antivirus, etc. Debe incluir el estatus de todos los túneles de VPNs, sitio a sitio y cliente a sitio.
1.122			La solución debe permitir la definición de umbrales y de las acciones a realizar cuando los mismos son alcanzados en los gateways. Las acciones deben incluir: LOGs, Alertas, traps SNMP, email y la ejecución de un script definido por el usuario. Debe incluir gráficos pre configurados para monitorear la evolución en el tiempo del tráfico y de los contadores del sistema: reglas de seguridad máximas, usuarios P2P, túneles VPNs, tráfico de red y otras informaciones útiles. Debe proveer la funcionalidad de generar nuevos gráficos personalizados usando diferentes tipos de tablas.
1.123			La solución debe proveer la capacidad de grabar las vistas de tráfico y de sistemas para visualización futura en cualquier momento. Debe ser capaz de reconocer el mal funcionamiento y los problemas de conectividad entre dos puntos conectados a través de un VPN, y crear logs y realizar alertas cuando un túnel VPN está abajo

1.124			La funcionalidad de correlación de eventos debe estar integrada totalmente en la aplicación de gerencia. Debe incluir herramientas para correlacionar eventos de todas las funcionalidades del gateway y de dispositivos y soluciones de terceros. Debe permitir la creación de filtros basados en cualquier característica de evento tales como aplicaciones de seguridad, direcciones IP origen y destino, servicio, tipo de evento, severidad, nombre del ataque, país de origen y destino, etc. Debe tener un mecanismo de asignación de estos filtros a diferentes gráficos de línea que puedan ser actualizados a intervalos regulares mostrando todos los eventos correspondientes a ese filtro, esto le permite al operador enfocarse en los eventos más importantes.
1.125			La funcionalidad de correlación de eventos debe suministrar una vista gráfica de los eventos basados en tiempo. Debe mostrar la distribución de eventos por países en un mapa. Debe permitir al administrador a agrupar los eventos basados en cualquiera de sus características incluyendo niveles de anidamiento y su exportación en formato PDF.
1.126			La funcionalidad debe incluir la opción de búsqueda dentro de la lista de eventos, y el drill down en los detalles para la investigación y análisis forénsico. Se debe incluir la funcionalidad de la creación de tablas gráficas con las características de los eventos.
1.127			La solución debe ser capaz de detectar ataques de Negación de Servicios correlacionando eventos de todas las fuentes. Debe detectar un login de administrador en horas irregulares. Debe detectar ataques de adivinación de credenciales. La solución debe reportar sobre todas las instalaciones de políticas de seguridad.
1.128			La solución debe incluir reportes predefinidos por hora, día, semana y mes incluyendo por lo menos los Eventos, Fuentes, Destinos, Servicios, Fuentes máximos, Fuentes máximas y sus eventos máximos, Destinos máximos y sus eventos máximos y los servicios máximos y sus eventos máximos. La herramienta de reportes debe permitir la aplicación de por lo menos 25 filtros que permitan personalizar los reportes predefinidos de acuerdo a las necesidades de los administradores
1.129			La herramienta de reportes debe soportar la calendarización automática de los reportes para la información que debe ser extraída de forma regular (día, semana, mes). La solución debe permitir al administrador definir la fecha y hora en que los reportes comienzan a generarse. Debe soportar formatos de reporte HTML, CSV y MHT. Debe soportar la distribución

			automáticas por email, la subida a servidores FTP/WEB y scripts personalizados de distribución de los mismos.
1.130			El sistema de reportes debe proveer información consolidada sobre: El volumen de conexiones que fueron bloqueadas por reglas de seguridad. Las fuentes máximas de las conexiones bloqueadas, su destino y servicios. Reglas máximas usadas por las políticas de seguridad por los puntos de enforzamiento (perímetro). Servicios de redes máximos. Actividad WEB por usuarios detallando los sitios más visitados y los mayores usuarios. Servicios máximos que crearon la mayor carga para el tráfico encriptado. Usuarios máximos de VPNs que realizan las conexiones de mayor duración.
1.131			La solución debe incluir un Portal de Gerencia con acceso basado en browser para visualizar en modo solo lectura las políticas de seguridad, manejar los logs de los firewalls y usuarios, proveyendo acceso a los gerentes y auditores sin la necesidad de usar la aplicación de gerencia. Esta solución debe incluir soporte SSL y puertos configurables.
1.132			La solución de Seguridad debe incluir una aplicación completamente integrada de Data Loss Prevention (DLT) que debe ser manejada de manera centralizada con las otras aplicaciones de seguridad de esta suite.
1.133			La aplicación de DLT debe tener mecanismos para el manejo de auto-incidentes de usuarios finales. Debe tener un mínimo de 500 tipos de data predefinidos. Debe poseer un lenguaje de creación de scripts para poder definir tipos de data relevantes a cada organización. Debe alertar al dueño del tipo de data cuando ocurre un incidente. Debe cubrir tipos de transporte SMTP, HTTP/HTTPS y protocolos FTP y TCP
1.134			La solución integrada de seguridad debe ofrecer una funcionalidad completa para asegurar los dispositivos móviles. Debe soportar tanto los dispositivos gerenciados como los no gerenciados tales como los BYOD.
1.135			La solución debe incluir todo el hardware, software, y licencias necesarias para poder manejar el siguiente dimensionamiento: Manejo de un Ancho de Banda Agregada de Acceso a Internet de por lo menos 500 Gbps y capacidad de crecimiento para por lo menos 1 Gbps. Capacidad de manejo de mínimo de 8 conexiones independientes a distintos proveedores de servicios. Configurada y licenciada para manejar un mínimo de 1200 end points, 1200 buzones de correo y 400 máquinas virtuales de servidores que pueden correr sistemas operativos Windows, Linux o Solaris

1.136			La solución debe tener un mínimo de 100 reglas de seguridad pre configuradas
1.137			La solución integrada debe ofrecer las siguiente soluciones de seguridad para todo este dimensionamiento : Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación de Amenazas y Extracción de Amenazas, VPNs IPsec, Data Loss Prevention
1.138			Las soluciones de Hardware deben ser ofertadas en clusters de alta disponibilidad con fuentes de poder y abanicos redundantes.
1.139			La solución debe ser capaz de trabajar de forma coordinada e integrada con la solución de seguridad de Sandboxing
2.000		***Expansión de la Solución de Web Application Firewall, Application Delivery, Balanceador y Protección de DDOS para Centro de Recuperación de Operaciones***	
2.001	1	***Expansión de la Solución de Web Application Firewall, Application Delivery, Balanceador y Protección de DDOS para Centro de Recuperación de Operaciones***	CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO
2.002			Los equipos ofertados debe ser una plataforma de hardware de propósito específico denominado "appliance".
2.003			El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.
2.004			Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado.
2.005			Se debe ofrecer dos (2) equipos en Alta disponibilidad funcionando en configuración de Par Activo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.
2.006			Cada equipo debe cumplir con las siguientes características:
2.007			La solución debe soportar un Throughput en L4 de al menos 20 Gbps

			La solución debe soportar un Throughput en L7 de al menos 20 Gbps
2.008			La solución debe soportar al menos 28 Millones de conexiones simultáneas La solución debe soportar al menos 250.000 conexiones por segundo en L4
2.009			La solución debe soportar al menos 1 Millón de HTTP Requests por Segundo Cada equipo debe contar con al menos las siguientes Interfaces de red: Al menos 8 puertos SFP a 1Gbps
2.010			Al menos 4 puertos SFP+ a 10 Gbps Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap) y certificadas 80 Plus Platinum" para eficiencia energética.
2.011			Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.
2.012			Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
2.013			Cada equipo debe incluir 32 Gb de Memoria RAM mínimo
2.014			Cada equipo debe incluir mínimo dos Disco duros de 500Gb en RAID 1
2.015			Debe soportar clúster Activo/Activo y Activo/Pasivo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).
2.016			La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda

2.017			Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.
2.018			Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.
2.019			La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
2.020			Los equipos deben tener hardware acelerador FPGA personalizables y programables para varias funciones como protección DDoS, protocolos SDN y manejo de trafico UDP
2.021			FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO
2.022			La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web (protocolos de capas superiores)
2.023			La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
2.024			La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
2.025			La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.
2.026			Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones
2.027			La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos

			deben realizarse de manera nativa y no por medio de configuración por scripting:
2.028			Round Robin Proporcional (Ratio)
2.029			Proporcional dinámico Respuesta más rápida
2.030			Conexiones mínimas Menor número de sesiones
2.031			Tendencia de menor cantidad de conexiones Tendencia de desempeño
2.032			Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM
2.033			El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)
2.034			El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
2.035			La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica
2.036			La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
2.037			Ping. Chequeo a nivel de TCP y UDP a puertos específicos
2.038			Monitoreo http y https Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.
2.039			Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. Ejecución de scripts para determinar la respuesta emulando un cliente.
2.040			Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.

			Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma
2.041			Monitoreo de aplicaciones de mercado: ○ LDAP ○ FTP ○ SMTP ○ IMAP/POP3 ○ Oracle ○ MSSQL ○ MySQL ○ RADIUS ○ SIP ○ Protocolo SASP ○ SOAP ○ WMI ○ SNMP Debe poder realizar todos estos métodos de persistencia de las conexiones: Dirección IP origen
2.042			Dirección IP destino Cookies
2.043			Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
2.044			Sesiones SSL Microsoft Remote Desktop
2.045			Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.
2.046			Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
2.047			El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.
2.048			Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:

2.049			Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados. Soporte de REST API Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts. Debe soportar el protocolo TDS para balanceo de MSSQL Debe soportar el protocolo NetFlow (v5 El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script. La solución debe permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código. El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3 Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline). Incluir el soporte de Aceleración SSL usando Hardware Dedicado FUNCIONES DE SEGURIDAD GENERALES Cada equipo debe soportar seguridad SSL con las

			siguientes características:
2.050			Incluir mínimo 10.000 Transacciones por segundo SSL (RSA 2K Keys) Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits
2.051			Soportar al menos 10 Gbps SSL Bulk Encryption (Thoughput SSL) Incluir mínimo 6.500 Transacciones por segundo SSL (ECDSA P-256)
2.052			La solución debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener la sesión SSL
2.053			El Stack TLS del equipo debe soportar las siguientes funcionalidades/características
2.054			Session ID Session Ticket

2.055			OCSP Stapling (on line certificate status protocol) Dynamic Record Sizing
2.056			ALPN (Application Layer Protocol Negotiation) Forward Secrecy
2.057			La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)
2.058			Debe soportar algoritmos de cifrado Camellia
2.059			El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall)
2.060			El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall
2.061			Firmado criptográfico de cookies para verificar su integridad.
2.062			Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto) Luna.
2.063			La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.
2.064			Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.
2.065			Debe soportar HSTS (HTTP Strict Transport Security)
2.066			Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.
2.067			Scanners Exploits Windows
2.068			Denial of Service Proxies de Phishing
2.069			Botnets Proxies anónimos
2.070			FUNCIONES DE ACELERACIÓN DE TRÁFICO

2.071			La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:
2.072			Memoria cache. Compresión tráfico HTTP
2.073			Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores
2.074			El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
2.075			Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 6 Gbps o superior usando aceleración por Hardware dedicado, no la CPU de propósito general.
2.076			Debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.
2.077			Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos
2.078			Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP
2.079			DNS Y BALANCEO A DE ENLACES DE INTERNET
2.080			La solución debe soportar el permitir alta disponibilidad de aplicaciones distribuidas en 2 o más Centro de Datoss, sin importar la ubicación geográfica.
2.081			Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.
2.082			Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.
2.083			Para el balanceo global (DNS), debe permitir los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting:
2.084			Round Robin Global Availability
2.085			Geolocalización Capacidad del Servicio

2.086			Least Connections Packets Per Second
2.087			Round Trip Time Drop Packet
2.088			Hops Packet Completion Rate
2.089			User-defined QoS Proporcional (Ratio)
2.090			Kilobytes Per Second Regreso al DNS
2.091			Persistencia estática Puntuación del Servicio
2.092			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo Centro de Datos por el transcurso de su sesión.
2.093			Permitir Balanceo de cargas ente Centro de Datoss de acuerdo a la ubicación geográfica
2.094			Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico basado en requerimientos particulares de la infraestructura
2.095			Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.
2.096			Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.
2.097			Debe permitir realizar balanceo de servidores DNS.
2.098			Debe soportar el protocolo DNSSEC
2.099			Debe incluir herramienta de administración grafica para el manejo de zonas DNS
2.100			Debe soportar registros AAAA para IPv6
2.101			Debe soportar traducción entre DNS IPv4 y DNS IPv6
2.102			La solución debe soportar 480.000 respuestas DNS por segundo.
2.103			La solución debe permitir balanceo de enlaces de internet, sin restringir el numero de enlaces y sin importar el proveedor de estos.
2.104			Debe proveer balanceo de tráfico saliente entre múltiples ISP y detectar el fallo de alguno de ellos para enrutar automáticamente el tráfico hacia los demás ISP.

2.105			Debe proveer balanceo de trafico entrante, basado en DNS y responder autoritativamente a queries DNS tipo A
2.106			Debe permitir monitoreo de los enlaces y detectar fallos en ellos.
2.107			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo ISP por el transcurso de su sesión
2.108			FUNCIONES DE FIREWALL Y PROTECCION DDOS
2.109			Debe incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables
2.110			La solución de DDoS debe contar con un sistema de protección basado en comportamiento (Behavioral) que permita la creación de firmas o vectores de ataque de manera dinámica.
2.111			La solución debe proteger contra ataques de denegación de servicio tanto en una topología en línea (inline deployment) como en una topología fuera de línea (TAP mode)
2.112			Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks
2.113			Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
2.114			Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.
2.115			Debe permitir la creación de reglas globales.
2.116			Debe tener la opción de funcionar como un firewall statefull full-proxy y ser certificado por ICSA Labs como Network Firewall
2.117			Debe permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas
2.118			Entre intervalos de tiempo
2.119			Hasta una fecha especifica
2.120			Después de una fecha específica.
2.121			Debe permitir la creación de listas blancas (White lists) de direcciones IP
2.122			Debe permitir la configuración de túnel IPSEC Site-to-Site
2.123			Debe incluir funcionalidad de application delivery controller o integrarse con dispositivos de Application Delivery
2.124			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y

			detectar anomalías a nivel del protocolo
2.125			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo
2.126			Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.
2.127			Debe funcionar como un Proxy SSH para control de conexiones entre diferentes redes con el fin de dar visibilidad a las sesiones SSH y controlar las mismas
2.128			Debe soportar Port Misuse, evitando que servicios pasando a través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).
2.129			Debe soportar RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.
2.130			Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT
2.131			ESTÁNDARES DE RED
2.132			Soporte VLAN 802.1q, Vlan tagging
2.133			Soporte de 802.3ad para definición de múltiples troncales
2.134			Soporte de NAT, SNAT
2.135			Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
2.136			Soporte de Rate Shapping.
2.137			Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
2.138			Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.
2.139			Debe soportar el protocol de OVSDB (Open vSwitch Database) para crear túneles VXLAN usando un controlador SDN
2.140			Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS

2.141			ADMINISTRACIÓN DEL SISTEMA
2.142			La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
2.143			La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
2.144			La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
2.145			La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
2.146			La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
2.147			La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
2.148			Protocolo SysLog Notificación vía SMTP
2.149			SNMP versión.2.0 o superior. El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico. El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque. La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos. Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas

			personalizadas que puedan ser actualizadas/exportadas entre equipos.
3.000		***Expansión de la Solución de Seguridad para la Estructura Virtual***	
3.001	***1***	***Expansión de la Solución de Seguridad para la Estructura Virtual, integrada con los Gateways de Manejo y Control de Seguridad Integrada redundantes. La solución actual está basada en equipos Checkpoint.***	Se requiere una expansión de la solución de seguridad integrada de los Gateways de Manejo y Control de Seguridad Integrada redundantes actuales, para el manejo de la Infraestructura Virtual del Ministerio. Esta Estructura virtual está basada en VMWare. La solución ofertada debe incluir todos los componentes necesarios, los servicios de configuración, implementación y puesta a punto de misma y Soporte Técnico y Mantenimiento de la misma por parte del fabricante por un período de 3 años con tiempo de respuesta NBD 8X5. La solución debe cumplir mínimo con los siguientes requerimientos técnicos:
3.002			La solución debe soportar la implementación con el Hipervisor de vCNS
3.003			La solución debe soportar la implementación con el Hipervisor de NSX
3.004			La solución debe soportar la importación de objetos virtuales directamente desde el Vcenter hacia las políticas de seguridad sin ninguna configuración manual en el vCenter y/o el NSX
3.005			La solución debe soportar la importación de Grupos de Seguridad directamente desde NSX hacia las políticas de seguridad
3.006			La solución debe permitir las conexión e importación de objetos virtuales desde mas de un NSX/vCenter
3.007			La solución debe ser capaz de manejar objetos virtuales in las políticas globales de seguridad de los dispositivos norte-sur incluso si redirecionar el tráfico a traves del NSX
3.008			La solución debe permitir la implementación de múltiples instancias de pasarelas de seguridad en el mismo host ESXi
3.009			La solución debe ser certificada y compatible con VMWare
3.010			La solución debe permitir las opciones de fallo-abierto/fallo-cerrado para cada instancia en caso de que no haya conectividad con Vcenter o NSX

3.011			La solución debe permitir la instalación de políticas de seguridad en las instancias virtuales antes de que el tráfico sea redireccionado en el NSX
3.012			La solución debe permitir la orquestación de las políticas de seguridad utilizando reglas de aprovisionamiento de auto-servicio
3.013			La solución debe tener creados los flujos de reglas de aprovisionamiento de las políticas de seguridad
3.014			La solución debe permitir que los administradores y orquestadores del data center utilicen automatización segura solo para políticas de seguridad específicas
3.015			La solución debe ofrecer desde el principio las capacidades de etiquetamiento de Máquinas Virtuales que permitan la actualización del NSX con los estados de seguridad de las acciones de automatización
3.016			La solución debe ofrecer el manejo unificado de las pasarelas de centro de datos tanto virtuales como físicas
3.017			La solución debe permitir la visualización de los nombre de los objetos en los logs de seguridad en adición a las direcciones IP de las Máquinas Virtuales
3.018			La solución debe tener sub-políticas dedicadas por micro-segmentos con privilegios de administración granulares
3.019			La solución debe soportar permisos dedicados para funciones y aplicaciones de niveles de políticas de seguridad específicos (Aplicaciones, Prevención de Amenazas, etc)
3.020			La solución debe ser capaz de tener visibilidad en las políticas de seguridad de las Máquinas Virtuales y los parametros de las mismas (IP, localización en el Centro de Datos, Sistema Operativo, etc)
3.021			Las redes virtuales deberán aprovisionar y administrar de forma programática, independientemente del hardware subyacente
3.022			Deberá permitir reproducir el modelo de red completo en Software, permitiendo la creación y aprovisionamiento de cualquier topología de red, desde redes simples hasta redes complejas de múltiples niveles
3.023			Deberá permitir reducir el tiempo de aprovisionamiento de redes, asi como permitir mejoras operacionales por medio de la automatización.
3.024			Deberá ser ompatible con overlays de redes basadas en LAN virtual extensible (Virtual eXtensible LAN, VXLAN).

3.025			Deberá permitir enrutamiento dinámico entre redes virtuales realizado de manera distribuida en el kernel del hipervisor, enrutamiento con escalabilidad horizontal y con conmutación de recuperación activo-activo, mediante enrutadores físicos.
3.026			Deberá soportar enrutamiento dinámico por medio de los protocolos BGP y OSPF así como enrutamiento estático.
3.027			Deberá tener la capacidad de conexión de VXLAN a redes físicas soportadas por VLAN para conexiones a cargas de trabajo físicas
3.028			Deberá ofrecer una Interface para el desarrollo de aplicaciones (API) tipo RESTful para la integración de cualquier plataforma de administración de nube o automatización.
3.029			Deberá incorporar las siguientes capacidades que soporten la operación de la plataforma: Interfaz de línea de Comandos Analizador de Trazas y flujos Analizador de puerto del switch (SPAN) Exportación de Flujos basado en IPFIX Integración con la herramienta de operaciones VMware vRealize Operations Integración con la herramienta vRealize Log Insight
3.030			La plataforma deberá ofrecer integración nativa con vRealize Automation y OpenStack
3.031			Automatización: Deberá permitir crear redes basadas en software, abordando los desafíos en el aprovisionamiento prolongado de redes, errores de configuración y procesos costosos, todo esto mediante el apovechamiento de la automatización
3.032			Deberá ofrecerse una plataforma para la seguridad y virtualización para ambientes VMware vSphere que funcione como Hipervisor de red
3.033			La plataforma deberá incorporar las siguientes funciones de red, incorporados directamente en el hipervisor ESXi y distribuídas en el entorno vSphere : Enrutamiento Conmutación de datos Protección de Firewall
3.034			Deberá suministrar micro-segmentación y seguridad granular y detallada para la carga de trabajo individual.
3.035			Deberá soportar protección de firewall distribuido e incorporado en el kernel del hipervisor para hasta 20 Gbps de capacidad de firewall por host hipervisor. La protección deberá ser sin pérdida del estado de las

			sesiones, lo anterior conocido como Stateful Firewall
3.036			En adición al firewall incorporado en el hipervisor, deberá soportar un Firewall para comunicacones Norte-Sur.
3.037			Deberá ofrecer capacidades de VPN tipo Sitio a Sitio
3.038			Deberá ofrecer capacidades de VPN de tipo Acceso Remoto
3.039			Las capacidades de micro-segmentación permitirán crear grupos de seguridad dinámicos y asociados con base a factores que van más allá de la dirección IP y MAC; dichos grupos deberán aprovechar los objetos y etiquedas de VMware vCenter, tipo de sistema operativo, información sobre aplicaciones de capa 7.
3.040			Seguridad: Deberá permitir dividir de manera lógica el centro de datos en distintos segmentos de seguridad hasta el nivel de la carga de trabajo individual, con independencia de la subred o VLAN, permitiendo definir políticas y controles de seguridad según los grupos de seguridad dinámicos, evitando el movimiento lateral dentro del Centro de Datos.
3.041			Deberá incorporar los siguientes elementos y servicios de red lógicos como parte de la misma plataforma: Switches Lógicos** Enrutamiento** Protección de Firewall Balaneo de Carga Red Privada Virtual (VPN) Calidad de Servicio (QoS) Monitoreo
3.042			Deberá permitir la movilidad de cargas de trabajo independiente de la topología de red física entre centros de datos y dentro de ellos.
3.043			Deberá soportar servicios de seguridad y de red avanzados a través de integraciones con terceros
3.044			Deberá permitir extensiones de overlay de la capa 2 lógica en una estructura de conexión enrutada (capa 3, C3) dentro de los límites del centro de datos y entre ellos.
3.045			El Firewall distribuido e incorporado en el kernel del hipervsor deberá ser compatible con Active Directory.
3.046			Deberá incorporar un servicio de Balanceo de Cargas de Capa 4 a Capa 7 (modelo OSI) con capacidad de

			descargar y transferencia de tráfico cifrado SSL.
3.047			El servicio de Balanceo de Cargas deberá tener la capacidad de comprobar el estado del servidior
3.048			El Servicio de Balanceo de Cargas deberá tener la capacidad de aplicar reglas de aplicación que permitan la programación y la manipulación del tráfico.
3.049			La plataforma deberá permitir integrarse con funciones del plano de control, plano de datos y administración con socios de terceros en distintas variedades como Firewalls de próxima generación, Sistemas de Detección de Intrusos (IDS), Sistemas de Prevención de Intrusos (IPS), Antivirus sin agentes, Controladores de suministro de aplicaciones, Conmutaciones, Operaciones y Visibilidad.
3.050			Deberá ofrecer la capacidad de extender la seguridad y las redes a través de los límites del centro de datos, con independencia de la topología física subyacente, lo que permitirá obtener capacidades como recuperación ante desastres y centros de datos Activo-Activo.
3.051			Continuidad de las aplicaciones: Deberá permitir replicar fácilmente entornos de aplicaciones completos en centros de datos remotos para la recuperación ante desastres, lo anterior mediante la separación de las redes del hardware subyacente, sin afectar el funcionamiento de las aplicaciones y sin tocar la red física.
3.052			Debe incorporar herramientas nativa para la gestión de reglas y monitoreo de terminales, para obtener una visualización integral de flujos de tráfico de red hasta la capa 7 del modelo OSI, permitiendo la identificación de terminales en el centro de datos y entre centros de datos y respondan mediante la creación de reglas de seguridad adecuadas
3.053			Se deben incluir y describir explícitamente 5 cupos de formación profesional oficiales, válidos para los esquemas de Certificación Profesional y avanzada de cada uno de los fabricantes, de cada una de las soluciones ofertadas. Estos cursos deben ofrecerse en la Ciudad de Santo Domingo y deben incluir toda la documentación y material de soporte de los mismos. En caso de no poder ser ofrecidos en la Ciudad de Santo Domingo, se deben incluir los costos de viáticos para los mismos.

2.9 Duración de los Bienes y Servicios

La Convocatoria al Procedimiento de Excepción de Proveedor Único se hace sobre la base de un suministro para un período de **tres (3) años**, contados a partir de la fecha de suscripción del contrato.

2.10 Programa de los Bienes y Servicios

Los pedidos se librarán en el lugar designado por la Entidad Contratante dentro del ámbito territorial de la República Dominicana y conforme al Cronograma de Entrega establecido.

2.11 Presentación de Propuestas Técnicas y Económicas "Sobre A" y "Sobre B"

Las Ofertas se presentarán en un Sobre cerrado y rotulado con las siguientes inscripciones:

NOMBRE DEL OFERENTE
(Sello social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda-PAFI
Referencia: PAFI-CCC-PEPU-2018-0010
Dirección: **Ave. México No. 45, Gazcue**
Teléfono: **809-687-5131 ext. 2436**

Este Sobre contendrá en su interior el **"Sobre A"** Propuesta Técnica y el **"Sobre B"** Propuesta Económica.

Ninguna oferta presentada en término podrá ser desestimada en el acto de apertura. Las que fueren observadas durante el acto de apertura se agregaran para su análisis por parte de los peritos designados.

2.12 Lugar, Fecha y Hora

La presentación de Propuestas **"Sobre A" y "Sobre B"** se efectuará en acto público, ante el Comité de Compras y Contrataciones y el Notario Público actuante, **en el Salón Matías Ramón Mella, sito Av. México No.45, Gazcue, el día lunes 01 de octubre del año 2018 desde las 8:00 hasta las 10:00 A.M, Apertura sobre "A" 11:30 AM.**, y sólo podrá postergarse por causas de Fuerza Mayor o Caso Fortuito definidos en el presente Pliego de Condiciones Específicas.

La Entidad Contratante no recibirá sobres que no estuviesen debidamente cerrados e identificados según lo dispuesto anteriormente.

2.13 Forma para la Presentación de los Documentos Contenidos en el "Sobre A"

Los documentos contenidos en el "Sobre A" deberán ser presentados en original debidamente marcado como **DOS (2) "ORIGINALES** en la primera página del ejemplar, junto con **UNA (1), fotocopia** simple de los mismos, debidamente marcada, en su primera página, como "COPIA". Las

originales y las copias deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

En adición a la presentación física de la Oferta Técnica del Sobre A, el Proponente deberá entregar una copia de la oferta en formato digital o magnético en archivo tipo PDF.

El "**Sobre A"** deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda-PAFI
PRESENTACIÓN: **OFERTA TÉCNICA**
REFERENCIA: PAFI-CCC-PEPU-2018-0010

2.14 Documentación a Presentar

A. Documentación Legal:
   1. Formulario de Presentación de Oferta **(SNCC.F.034)**;
   2. Formulario de Información sobre el Oferente **(SNCC.F.042)**;
   3. Copia de los Estatutos Sociales del oferente participante, en caso de ser un oferente constituido bajo las leyes de la República Dominicana los indicados Estatutos deberán estar conforme a la Ley No. 479-08, de fecha 11 de diciembre de 2008, sobre las Sociedades Comerciales y Empresas Individuales de Responsabilidad Limitada y sus modificaciones;
   4. Copia legible, vigente y actualizada del Certificado de Registro Mercantil o equivalente del oferente, donde conste que se dedica(n) a la actividad comercial del ámbito de la licitación;
   5. Copia de la última Acta de Asamblea y Nómina de Presencia del oferente;
   6. Constancia de inscripción en el Registro de Proveedores del Estado (RPE) en donde el oferente acredite su inscripción en un rubro de la actividad comercial requerida para participar en esta licitación. En el caso de un oferente extranjero, no necesitará estar registrado en el RPE, salvo el caso de que se encuentre domiciliado en la República Dominicana. Sin embargo, si resulta adjudicatario, previa suscripción del contrato, deberá obtener y depositar el registro correspondiente, según lo establecido en los artículos del 21 al 25 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la precitada Ley No. 340-06.

      El Registro de Proveedores del Estado (RPE) deberá estar actualizado conforme lo establece el artículo 19 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la Ley No. 340-06 y sus modificaciones, así como la Resolución No. 14-2015, de fecha 27 de enero de 2015, dictada por la Dirección General de Contrataciones Públicas;

7. El oferente nacional o extranjero, aún se encuentre inscrito en el Registro de Proveedores del Estado (RPE), deberá presentar una (1) declaración simple en original, en las que se haga constar lo siguiente:

    a) Que el oferente no se encuentra afectado por las prohibiciones establecidas en el artículo 14 de la Ley No. 340-06 y sus modificaciones, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones.
    b) Que el oferente tiene o no juicios con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no Financieras, y de las Instituciones Públicas de la Seguridad Social.

    El oferente deberá utilizar el modelo de declaración simple que dispone la Dirección General de Contrataciones Públicas, para estos fines;

8. Certificación actualizada y legible de la Dirección General de Impuestos Internos (DGII) o en su defecto del organismo que en el país de origen del Oferente (si éste no se encuentra domiciliado y/o legalmente representado en la República Dominicana) sea el que determine que se encuentra al día en el pago de sus obligaciones fiscales;
9. Certificación de pago de la Tesorería de la Seguridad Social (TSS) del oferente. En el caso de un oferente extranjero, este requisito sólo aplicará cuando dicho oferente se encuentre domiciliado y/o legalmente representado en la República Dominicana;
10. Poder de Representación otorgado ante Notario Público Nacional o copia del Acta de la Asamblea del Consejo de Administración o de la Asamblea General de Accionistas u Socios, según sea el caso. Si la sociedad comercial participante está representada por su Presidente o Gerente, y siempre y cuando los Estatutos Sociales le otorguen el Poder de Representación de la sociedad, no es necesario presentar este requerimiento;
11. Copia legible y vigente de la Cédula de Identidad y Electoral del Representante Legal. En caso de ser extranjero con residencia, depositará copia legible y vigente de la Cédula de Identidad o Pasaporte si no reside en el país.

B. Documentación Financiera:
    a. Estados Financieros de los **dos (2)** últimos ejercicios contables consecutivos.

C. Documentación Técnica:
    a. Oferta Técnica (conforme a las especificaciones técnicas suministradas)
    b. Formulario de Entrega de Muestra (SNCC.F.056).
    c. Autorización del Fabricante y/o Representante en los casos de que los Bienes y Servicios conexos no sean fabricados por el Oferente (SNCC.F.047).

Para los consorcios:

En adición a los requisitos anteriormente expuestos, los consorcios deberán presentar:

1. Original del Acto Notarial por el cual se formaliza el consorcio, incluyendo su objeto, las obligaciones de las partes, su duración la capacidad de ejercicio de cada miembro del consorcio, así como sus generales.
2. Poder especial de designación del representante o gerente único del Consorcio autorizado por todas las empresas participantes en el consorcio.

2.15 Presentación de la Documentación Contenida en el "Sobre B"

A) **Formulario de Presentación de Oferta Económica (SNCC.F.33),** presentado en **Dos (2)** originales debidamente marcados como "**ORIGINALES**" en la primera página de la Oferta, junto con **una (1)** fotocopia simple de la misma, debidamente marcada, en su primera página, como "**COPIA**". El original y las copias deberán estar firmados en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

B) **Garantía de la Seriedad de la Oferta.** Correspondiente a **Póliza de Fianza o Garantía Bancaria.** La vigencia de la garantía deberá ser igual al plazo de validez de la oferta establecido en el numeral 3.8 del presente Pliego de Condiciones.

El **"Sobre B"** deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda-PAFI
PRESENTACIÓN: **OFERTA ECONÓMICA**
REFERENCIA: PAFI-CCC-PEPU-2018-0010[3]

Las Ofertas deberán ser presentadas únicas y exclusivamente en el formulario designado al efecto, **(SNCC.F.033)**, **siendo inválida toda oferta bajo otra presentación**.

La Oferta Económica deberá presentarse en Pesos Dominicanos (RD$). Los precios deberán expresarse en **dos decimales (XX.XX)** que tendrán que incluir todas las tasas (divisas), impuestos y gastos que correspondan, transparentados e implícitos según corresponda.

El Oferente será responsable y pagará todos los impuestos, derechos de aduana, o gravámenes que hubiesen sido fijados por autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los bienes y servicios conexos a ser suministrados.
Ninguna institución sujeta a las disposiciones de la Ley que realice contrataciones, podrá contratar o convenir sobre disposiciones o cláusulas que dispongan sobre exenciones o exoneraciones de impuestos y otros atributos, o dejar de pagarlos, sin la debida aprobación del Congreso Nacional.

El Oferente/Proponente que cotice en cualquier moneda distinta al Peso Dominicano (RD$), **se auto-descalifica para ser adjudicatario.**

A fin de cubrir las eventuales variaciones de la tasa de cambio del Dólar de los Estados Unidos de A fin de cubrir las eventuales variaciones de la tasa de cambio del Dólar de los Estados Unidos de Norteamérica (US$), **el Programa de Administración Financiera Integrada (PAFI) del Ministerio**

[3] **La referencia corresponde al nombre de la institución- Comité de Compras y Contrataciones - Procedimiento de Excepción de Proveedor Único- Año- número secuencial de procedimientos llevados a cabo.**

de Hacienda, podrá considerar eventuales ajustes, una vez que las variaciones registradas sobrepasen el **cinco por ciento (5%)** con relación al precio adjudicado o de última aplicación. La aplicación del ajuste podrá ser igual o menor que los cambios registrados en la Tasa de Cambio Oficial del Dólar Americano (US$) publicada por el Banco Central de la República Dominicana, a la fecha de la entrega de la Oferta Económica.

En el caso de que el Oferente/Proponente Adjudicatario solicitara un eventual ajuste, **el Programa de Administración Financiera Integrada (PAFI) del Ministerio de Hacienda,** se compromete a dar respuesta dentro de los siguientes **cinco (5) días laborables**, contados a partir de la fecha de acuse de recibo de la solicitud realizada.

La solicitud de ajuste no modifica el Cronograma de Entrega de Cantidades Adjudicadas, por lo que, el Proveedor Adjudicatario se compromete a no alterar la fecha de programación de entrega de los Bienes y Servicios conexos pactados, bajo el alegato de esperar respuesta a su solicitud.

Los precios no deberán presentar alteraciones ni correcciones y **deberán ser dados en la unidad de medida establecida en el Formulario de Oferta Económica.**

En los casos en que la Oferta la constituyan varios bienes, solo se tomará en cuenta la cotización únicamente de lo evaluado CONFORME en el proceso de evaluación técnica.

Será responsabilidad del Oferente/Proponente la adecuación de los precios unitarios a las unidades de medidas solicitadas, considerando a los efectos de adjudicación el precio consignado en la Oferta Económica como el unitario y valorándolo como tal, respecto de otras Ofertas de los mismos productos. El Comité de Compras y Contrataciones, no realizará ninguna conversión de precios unitarios si éstos se consignaren en unidades diferentes a las solicitadas.

Sección III
Apertura y Validación de Ofertas

3.1 Procedimiento de Apertura de Sobres

La apertura de Sobres se realizará en acto público en presencia del Comité de Compras y Contrataciones y del Notario Público actuante, en la fecha, lugar y hora establecidos en el Cronograma del Procedimiento de Excepción de Proveedor Único.

Una vez pasada la hora establecida para la recepción de los Sobres de los Oferentes/Proponentes, no se aceptará la presentación de nuevas propuestas, aunque el acto de apertura no se inicie a la hora señalada.

3.2 Apertura de "Sobre A", contentivo de Propuestas Técnicas

El Notario Público actuante procederá a la apertura de los "**Sobres A"**, según el orden de llegada, procediendo a verificar que la documentación contenida en los mismos esté correcta de conformidad con el listado que al efecto le será entregado. El Notario Público actuante, deberá rubricar y sellar

cada una de las páginas de los documentos contenidos en los "**Sobres A"**, haciendo constar en el mismo la cantidad de páginas existentes.

En caso de que surja alguna discrepancia entre la relación y los documentos efectivamente presentados, el Notario Público autorizado dejará constancia de ello en el acta notarial.

El Notario Público actuante elaborará el acta notarial correspondiente, incluyendo las observaciones realizadas en el desarrollo del acto de apertura de los Sobres A, si las hubiere.
El Notario Público actuante concluido el acto de recepción, dará por cerrado el mismo, indicando la hora de cierre.

Las actas notariales estarán disponibles para los Oferentes/ Proponentes, o sus Representantes Legales, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.3 Validación y Verificación de Documentos

Los Peritos, procederá a la validación y verificación de los documentos contenidos en el referido "**Sobre A".** Ante cualquier duda sobre la información presentada, podrá comprobar, por los medios que considere adecuados, la veracidad de la información recibida.

No se considerarán aclaraciones a una Oferta presentadas por Oferentes cuando no sean en respuesta a una solicitud de la Entidad Contratante. La solicitud de aclaración por la Entidad Contratante y la respuesta deberán ser hechas por escrito.

Antes de proceder a la evaluación detallada del "**Sobre A",** los Peritos determinarán si cada Oferta se ajusta sustancialmente al presente Pliego de Condiciones Específica; o si existen desviaciones, reservas, omisiones o errores de naturaleza o de tipo subsanables de conformidad a lo establecido en el numeral 1.21 del presente documento.

En los casos en que se presenten desviaciones, reservas, omisiones o errores de naturaleza o tipo subsanables, los Peritos Especialistas procederán de conformidad con los procedimientos establecidos en el presente Pliego de Condiciones Específicas.

3.4 Criterios de Evaluación

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar los siguientes aspectos que serán verificados bajo la modalidad **"CUMPLE/ NO CUMPLE":**
Elegibilidad: Que el Proponente está legalmente autorizado para realizar sus actividades comerciales en el país.

Capacidad Técnica: Que los Bienes y Servicios conexos cumplan con las todas características especificadas en las Fichas Técnicas.

La evaluación y calificación de las propuestas se realizará mediante las siguientes matrices:

- Tabla de Evaluación Legal
- Tabla de Evaluación Financiera
- Tabla de Evaluación Técnica

Ministerio de Hacienda de la República Dominicana			
Evaluación legal			
Ampliación de las plataformas de Hardware y Software para el Almacenamiento y Procesamiento de los aplicativos y bases de datos del Ministerio de Hacienda.			
No.	**Documentos legales**	**CUMPLE**	**NO CUMPLE**
1	Formulario de Presentación de Oferta (SNCC.F.034);		
2	Formulario de Información sobre el Oferente (SNCC.F.042);		
3	Copia de los Estatutos Sociales del oferente participante, en caso de ser un oferente constituido bajo las leyes de la República Dominicana los indicados Estatutos deberán estar conforme a la Ley No. 479-08, de fecha 11 de diciembre de 2008, sobre las Sociedades Comerciales y Empresas Individuales de Responsabilidad Limitada y sus modificaciones;		
4	Copia legible, vigente y actualizada del Certificado de Registro Mercantil o equivalente del oferente, donde conste que se dedica(n) a la actividad comercial del ámbito de la licitación;		
5	Copia de la última Acta de Asamblea y Nómina de Presencia del oferente		
6	Constancia de inscripción en el Registro de Proveedores del Estado (RPE) en donde el oferente acredite su inscripción en un rubro de la actividad comercial requerida para participar en esta licitación. En el caso de un oferente extranjero, no necesitará estar registrado en el RPE, salvo el caso de que se encuentre domiciliado en la República Dominicana. Sin embargo, si resulta adjudicatario, previa suscripción del contrato, deberá obtener y depositar el registro correspondiente, según lo establecido en los artículos del 21 al 25 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la precitada Ley No. 340-06. El Registro de Proveedores del Estado (RPE) deberá estar actualizado conforme lo establece el artículo 19 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la Ley No. 340-06 y sus modificaciones, así como la Resolución No. 14-2015, de fecha 27 de enero de 2015, dictada por la Dirección General de Contrataciones Públicas;		
7	El oferente nacional o extranjero, aún se encuentre inscrito en el Registro de Proveedores del Estado (RPE), deberá presentar una (1) declaración simple en original, en las que se haga constar lo siguiente: a) Que el oferente no se encuentra afectado por las prohibiciones establecidas en el artículo 14 de la Ley No. 340-06 y sus modificaciones, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones. b) Que el oferente tiene o no juicios con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no Financieras, y de las Instituciones Públicas de la Seguridad Social. El oferente deberá utilizar el modelo de declaración simple que dispone la Dirección General de Contrataciones Públicas, para estos fines;		

8	Certificación actualizada y legible de la Dirección General de Impuestos Internos (DGII) o en su defecto del organismo que en el país de origen del Oferente (si éste no se encuentra domiciliado y/o legalmente representado en la República Dominicana) sea el que determine que se encuentra al día en el pago de sus obligaciones fiscales		
9	Certificación de pago de la Tesorería de la Seguridad Social (TSS) del oferente. En el caso de un oferente extranjero, este requisito sólo aplicará cuando dicho oferente se encuentre domiciliado y/o legalmente representado en la República Dominicana		
10	Poder de Representación otorgado ante Notario Público Nacional o copia del Acta de la Asamblea del Consejo de Administración o de la Asamblea General de Accionistas u Socios, según sea el caso. Si la sociedad comercial participante está representada por su Presidente o Gerente, y siempre y cuando los Estatutos Sociales le otorguen el Poder de Representación de la sociedad, no es necesario presentar este requerimiento;		
11	Copia legible y vigente de la Cédula de Identidad y Electoral del Representante Legal. En caso de ser extranjero con residencia, depositará copia legible y vigente de la Cédula de Identidad o Pasaporte si no reside en el país		

Ministerio de Hacienda de la República Dominicana			
Evaluación Financiera			
Ampliación de las plataformas de Hardware y Software para el Almacenamiento y Procesamiento de los aplicativos y bases de datos del Ministerio de Hacienda.			
No.	**Documentos Financieros**	**CUMPLE**	**NO CUMPLE**
	a. Estados Financieros de los dos (2) últimos ejercicios contables consecutivos		

Ministerio de Hacienda de la República Dominicana					
Términos de Referencia Técnicos					
Ampliación de las Soluciones de Web Application Firewall, Application Delivery, Balanceo de Aplicaciones y Protección de DDOS; Gateways de Manejo y Control de Seguridad Integrada y Software de Seguridad para la Infraestructura de Virtualización del Ministerio de Hacienda.					
NO Partida	**Cantidad**	***Descripción***	**Evaluación Técnica**		
			Especificaciones Técnicas	**CUMPLE**	**NO CUMPLE**
1.000		***Expansión de la Solución de Gateways de Manejo y Control de Seguridad Integrada redundantes para Firewall.***			
1.001	***1***	***Expansión de la Solución de Gateways de Manejo y Control de Seguridad Integrada redundantes para Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación y Extracción de Amenazas, VPNs Ipsec, Data Loss Prevention e integración con la solución de Sandboxing. La solución actual está***	Los Gateways de Manejo y Control de Seguridad Integrada redundantes deben estar configurados en un esquema de alta disponibilidad con fuentes de poder y abanicos de enfriamiento redundantes y deben cumplir con un mínimo de las siguientes configuraciones y ser capaces de manejar los siguientes aspectos de seguridad cada uno:		

		basada en equipos Checkpoint.			
1.002			115 Gbps de Throughput de Firewall 20 Gbps de Throughput de IPS 20 Gbps de Throughput de Next Generation Firewall 15 Gbps de Throughput de Threat Prevention Discos Duros SSD redundantes con un mínimo de 450 GB cada uno Cinco (5) slots de expansión para tarjetas de interfases de redes Puerto de Consola, Puerto para Gerencia Lights Out, Puerto de Gerencia 10/100/1000 RJ45 10 puertos de Conexiones a 10/100/1000 RJ45 10 puertos de Conexiones a 10 Gbps SFP+ con los Módulos de Conexión de Fibra Óptica Multimodo 2 puertos de Conexión a 40 Gbps QSFP+ con los Módulos de Conexión de Fibra Óptica Multimodo		
1.003			Debe ser capaz de soportar, estar configurada y licenciada para manejar un mínimo de 10 firewalls virtuales. Debe soportar control de acceso para por lo menos 150 servicios y/o protocolos predefinidos		
1.004			Debe permitir definir reglas de seguridad que puedan ser enforzadas dentro de intervalos de tiempo configurados con tiempo y fecha de expiración. Debe manejar estadísticas de conteo de la utilización de cada una de las reglas de seguridad y enviar las mismas a la aplicación de gerencia de la aplicación.		
1.005			Debe soportar métodos de autenticación basados en clientes, usuarios y sesiones.		
1.006			La comunicación entre los servidores de gerencia y los Gateways de Seguridad deben ser encriptados y autenticados con Certificados PKI		
1.007			Debe soportar DCHP, server y relay. Debe incluir una base de datos de usuarios local que permita la autenticación y autorización sin necesidad de ningún dispositivo externo.		
1.008			Deben soportarse los siguientes esquemas de autenticación de usuarios: Tokens (SecureID), TACACS, RADIUS y Certificados Digitales		
1.009			Debe soportar y estar configurada en Alta Disponibilidad en los Gateways con balanceo de carga y sincronización de estado. Debe ser capaz de trabajar en modo Bridge/Transparente y soportar HTTP y proxy PTTPS		
1.010			Debe soportar la configuración de gateways en stacks dobles o con un interfase de unión o como una sub-interfase de un interfase de unión.		

1.011			Debe soportar tráfico IPv6 en los módulos de IPS, APP, Firewall, Identity Awareness, filtrado URL, Antivirus y Anti BOT. Debe soportar NAT 6 a 4, o túneles 6 a 4. Debe soportar integración AD usando tráfico IPv6		
1.012			Debe soportar seguimiento y logs que muestren el tráfico IPv6. Debe soportar la habilidad de mostrar tablas de ruteo IPv6.		
1.013			La solución debe soportar los siguientes RFCs IPv6:		
1.014			RFC 1981 Path Maximum Transmission Unit Discovery for IPv6		
1.015			RFC 2460 IPv6 Basic specification		
1.016			RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
1.017			RFC 3596 DNS Extensions to support IPv6		
1.018			RFC 4007 IPv6 Scoped Address Architecture		
1.019			RFC 4193 Unique Local IPv6 Unicast Addresses		
1.020			RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.		
1.021			RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)		
1.022			RFC 4443 ICMPv6		
1.023			RFC 4861 Neighbor Discovery		
1.024			RFC 4862 IPv6 Stateless Address Auto-configuration		
1.025			La solución de IPS debe mínimamente permitir los mecanismos de detección basados en exploit signatures, anomalías de protocolos, y detección por el control y el comportamiento de las aplicaciones		
1.026			La solución debe pertenecer al cuadrante de líderes del Cuadrante Mágico de Gartner para las soluciones de Firewall e IPS		
1.027			Las soluciones de IPS y de Firewall deben estar integradas en una única plataforma		
1.028			La administración de la solución de IPS debe permitir que se configure la inspección para proteger solamente los hosts internos. El IPS debe tener las opciones de crear perfiles para protección de clientes, servidores o una combinación de ambos.		
1.029			La solución de IPS debe proveer pre configurada por lo menos dos perfiles y/o políticas que puedan ser usadas de forma inmediata		

1.030			Los IPS deben tener un mecanismo basado en fail-open que pueda ser configurado en base a límites del uso de la memoria y los CPUs de los Gateways		
1.031			Los IPS deben ser capaces de activar o manejar mecanismos automáticos de nuevas firmas desde las actualizaciones. Deben soportar excepciones de redes basadas en la fuente, el destino, el servicio o una combinación de las tres anteriores.		
1.032			Los IPS deben incluir una modalidad de Troubleshooting que permita al perfil en uso que solo detecte sin modificar las protecciones individuales		
1.033			La solución de IPS debe tener un mecanismo centralizado de correlación y reporte de eventos. El administrador debe ser capaz de activar automáticamente nuevas protecciones basadas en parámetros configurables tales como impacto de rendimiento, severidad de las amenazas, niveles de confianza, protecciones a los clientes y protecciones a los servidores.		
1.034			La solución de IPS debe se capaz de detectar y prevenir las amenazas siguientes: Mal uso de protocolos, comunicaciones de Malware, intentos de uso de túneles, y tipos de ataques genéricos sin firmas predeterminadas. Para cada protección, la solución debe incluir tipos de protección para clientes y servidores, severidad de las amenazas, impacto en el rendimiento, niveles de confianza y referencias de la industria.		
1.035			Los IPS deben ser capaces de recolectar capturas de paquetes para protecciones específicas. Deben ser capaces de detectar y bloquear ataques a niveles de red y de aplicaciones, protegiendo un mínimo de los siguientes servicios: email, DNS, FTP, y Servicios de Windows (Microsoft Networking). La solución debe ser líder protegiendo las vulnerabilidades de Microsoft		
1.036			Los IPS y los controles de aplicaciones deben incluir la habilidad para detectar y bloquear aplicaciones P2P y evasivas. El administrador debe ser capaz de definir las redes y los hosts a ser excluidos de la inspección de los IPS		
1.037			Los IPS deben proteger del Envenenamiento del Cache del DNS y prevenir a los usuarios de accesar las direcciones de dominios bloqueados. Debe proveer protección a los protocolos de VOIP		
1.038			Los IPS y los controles de aplicaciones deben detectar y bloquear las aplicaciones de control remoto, incluyendo aquellas que son capaces de manejar túneles sobre tráfico HTTP. Deben incluir protección a protocolos SCADA y tener un mecanismo para convertir firmas SNORT.		

1.039			La solución debe poder enforzar los protocolos de Citrix. Debe permitir al administrador a bloquear fácilmente el tráfico outbound o inbound basado en los Paises, sin necesidad de manejar manualmente rangos de direcciones IP correspondientes a esos países.		
1.040			La solución de Adquisición de la Identidad del Usuario debe ser capaz de adquirir la identidad del usuario solicitando la misma al Microsoft Active Directory basada en los eventos de seguridad		
1.041			Debe ofrecer un método de Autenticación de Identidad de Usuario basado en browser para los usuarios o activos que no pertenecen a dominio. Debe tener un agente de cliente dedicado que pueda ser instalado por políticas en las computadoras de los usuarios que puedan adquirir y reportar las identidades a los Gateways de Seguridad		
1.042			Debe soportar ambientes de terminal servers. Debe integrarse de forma nativa con servicios de directorios, IF-MAP y RADIUS		
1.043			El impacto de estos servicios debe ser menor al 3% en los controladores de dominio. La solución debe soportar terminales y servidores Citrix		
1.044			La solución debe permitir la identificación a través de un proxy. Debe ser capaz de adquirir la identidad del usuario del Microsoft Active Directory sin necesidad de instalar ningún agente en los controladores de dominio.		
1.045			Debe soportar autenticación transparente de Kerberos mediante un sign on único. Debe soportar el uso de grupos anidados de LDAP. Debe ser capaz de compartir y propagar identidades de usuarios entre múltiples gateways de seguridad y crear roles de identidad que puedan ser usados a través de todas las aplicaciones de seguridad		
1.046			La base de datos de la Solución para Control de Aplicaciones y Filtrado de URL debe contener más de 6000 aplicaciones conocidas. Debe tener una categorización de URLs que contenga mas de 200 millones de URLs y que cubra más del 85% del millón de sitios topes de Alexa		
1.047			La solución debe ser capaz de crear reglas de filtrado con múltiples categorías. Debe ser capaz de crear filtros para un único site.		
1.048			Debe tener granularidad de usuarios y grupos para las reglas de seguridad.		
1.049			Los Caches locales de los Gateways de Seguridad deben ser capaces de ofrecer respuestas al 99% de los requerimientos de categorizaciones de los URLs dentro de las primeras 4 semanas luego de la entrada en producción de los mismos		

1.050			Debe poseer un interfase fácil, que permita búsquedas para las aplicaciones y los URLs. La solución debe ser capaz de categorizar las aplicaciones y los URLs en base a Factores de Riesgo. El control de las aplicaciones y las políticas de seguridad de los URLF debe ser capaz de ser definido en base a las identidades de los usuarios.		
1.051			El control de las aplicaciones y la base de datos de URLF debe ser capaz de ser actualizados mediante servicios en la nube. Debe poder manejar reglas unificadas para el control de aplicaciones y de URLF		
1.052			La solución debe proveer mecanismos para informar o preguntar a los usuarios en tiempo real para educarlos o confirmar acciones basadas en las políticas de seguridad.		
1.053			La solución debe ser capaz de proveer un mecanismo para limitar el uso de aplicaciones basado en el consumo de ancho de banda de las mismas. Debe permitir excepciones de redes basadas en objetos de redes definidos.		
1.054			La Solución debe proveer opciones de modificar la Notificación de Bloqueo y re direccionar al usuario a una página de remediación. Debe incluir mecanismos de Listas Blancas y Negras, y permitir al administrador negar o permitir acceso a URLs específicas independientemente de las categorías.		
1.055			La solución debe tener mecanismos configurables de Bypass. Debe proveer un mecanismo de override para la categorización de la base de datos de URLS.		
1.056			El control de las aplicaciones y las políticas de seguridad de los URLF deben reportar el conteo de usos de las reglas		
1.057			La solución debe incluir las aplicaciones de Anti-BOT y Anti-Virus integradas en los Gateways de Seguridad.		
1.058			La aplicación de Anti-BOT debe ser capaz de detectar y detener comportamientos anormales o sospechosos de la red. Debe utilizar un motor de detección de multi-niveles que incluya la reputación de las direcciones Ips, los URLs y las Direcciones de DNS y que detecte patrones de comunicaciones de BOTs. Las protecciones Anti-BOT deben ser capaces de realizar búsquedas de acciones de BOT.		
1.059			La solución debe soportar la detección y prevención de virus tipo Cryptors y Ransomware y sus variantes mediante análisis dinámicos y/o estáticos. Debe ser capaz de proteger contra ataques tipo spear phishing.		
1.060			Debe poseer capacidades de detección y prevención de C&C DNS hide outs. Debe ser capaz de determinar patrones de tráfico C&C, no solo en su destino de DNS		

1.061			Debe ser capaz de realizar ingeniería de reversa para descubrir su DGA (Domain Name Generation). Debe poseer características para manejar traps de DNS para la prevención de amenazas y asistencia en el descubrimiento de hosts infectados que generan comunicaciones C&C. Debe tener capacidades de detección y prevención para proteger de ataques mediante túneles de DNS		
1.062			Las políticas de Anti-BOT y Anti-Virus deben poder administrarse desde una consola central. Las aplicaciones de Anti-BOT y Anti-Virus deben tener un mecanismo centralizado de correlación y reportes de eventos.		
1.063			La aplicación de Anti-Virus debe ser capaz de prevenir acceso a websites maliciosos e inspeccionar tráfico SSL encriptado. Debe ser capaz de detener archivos maliciosos de entrada. Debe poder escanear archivos almacenados.		
1.064			Las soluciones de Anti-BOT y Anti-Virus deben recibir actualizaciones en tiempo real de servicios de reputación basados en la nube. Deben ser capaces de manejar políticas de configuración y enforzamiento granulares de manera centralizada.		
1.065			El Anti-Virus debe soportar mas de 50 motores de Anti-Virus basados en la nube. Debe soportar escaneo de links dentro de los emails y escanear archivos que están pasando mediante el protocolo CIFS		
1.066			La solución debe incluir la Inspección SSL tanto de tráfico entrante como saliente. Debe soportar la Inspección/Decriptamiento con rendimiento líder a través de todas las tecnologías de mitigación		
1.067			Debe soportar Perfect Forward Secrecy (PFS, ECDHE conjuntos de cifrado), y AES-NI, AES-GCM para mejoras en el flujo		
1.068			Deben incluirse funcionalidades para la emulación de amenazas y sandboxing integradas a la inspección de SSL.		
1.069			La solución debe aprovechar la base de datos de filtrado de URLs para permitirle al administrador crear políticas de inspección de URLs granulares. Debe ser capaz de inspeccionar filtrado de URLs basado en HTTPS sin requerir decripción SSL		
1.070			La solución debe ofrecer la funcionalidad de coordinación e integración con soluciones de Emulación de Amenazas (Sandboxing).		

1.071			Debe proveer la habilidad de proteger contra ataques de malware y Zero-Day antes de que las protecciones de firmas estáticas hayan sido creadas. Deben proveer prevención en tiempo real de malware de Paciente-0 en Web Browsing y email		
1.072			La Solución de Seguridad debe ser una arquitectura de prevención de amenazas completa y multinivel con mínimo de funcionalidades de: IPS, AV, AB, URLF, APP FW		
1.073			La Solución de Seguridad debe soportar emulación de amenazas basada en Redes y Hosts. Debe ser capaz de soportar implementaciones basadas en sitio y en la nube. Se debe incluir en esta propuesta la integración con una solución basada en hosts locales instalados en las premisas de la institución		
1.074			La solución debe soportar integración de terceros mediante APIs públicos. Debe soportar implementación en modo Inline, MTA (Mail Transfer Agent), inspect TLS y SSL. Debe soportar implementación en modo de puerto TAP/SPAN		
1.075			La solución no debe requerir infraestructura separada para protección de email y protección de WEB.		
1.076			Los dispositivos deben soportar instalación en Clusters de alta disponibilidad y deben estar configurados y ofertados en este esquema		
1.077			La solución debe ser capaz de emular archivos almacenados ejecutables, documentos JAVA y FLASH, específicamente:		
1.078			7z, cab,csv,doc, docm, docx,dot,dotm, exe, jar, pdf, potx,pps, ppsm, ppsx, ppt, pptm, pptx,rar, rtf, scr,swf,tar, xla,xls,xlsb, xlsm,xlsx,xlt,xltm,xltx,xlw,zip,pif,com,gz,bz2,tgz,apk,ipa,ISO,js,cpl,vbs,jse,vba,bve,wsf,wsh		
1.079			La solución debe ser capaz de emular ejecutables, archivos almacenados, documentos, JAVA y Flash específicamente dentro de los siguientes protocolos:		
1.080			HTTP,HTTPS,FTP,SMTP,CIFS(SMB), SMTP TLS		
1.081			El motor de emulación debe soportar múltiples sistemas operativos tales como Windows 7,8,10 a 32/64 gbits incluyendo imágenes customizadas. La solución debe ofrecer el soporte de licencias prepopuladas de copias de imágenes Microsoft Windows y Office mediante un acuerdo con Microsoft		
1.082			El motor de la solución debe detectar llamados a APIs, cambios en los archivos del sistema, los registros, las conexiones de redes y los procesos del sistema. Debe soportar análisis estático para Windows, mac OS-X, Linux o cualquier plataforma x86		

1.083			El motor de emulación de la tecnología de Sandboxing debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing en la infraestructura de anti-malware		
1.084			La solución debe ser capaz de realizar filtrado estático pre-emulación. La solución debe permitir la emulación de archivos de un tamaño mayor de 10Mb en todos los tipos soportados. Debe soportar motores de detección basados en aprendizaje automático de máquinas.		
1.085			La solución debe detectar el ataque en el nivel de explotación, es decir, antes que el código Shell sea ejecutado y antes que el malware sea bajado/ejecutado. Debe ser capaz de detectar los ROP y otras técnicas de explotación tales como escalación de privilegios monitoreando el flujo del CPU		
1.086			La solución debe ser capaz de soportar links de escaneo dentro de los emails para malwares desconocidos y de Día0. Debe ser capaz de escanear los URLS históricos almacenados los últimos X días y comprobar si los ratings han cambiado, por ejemplo, de rating limpio a malicioso.		
1.087			El tiempo de emulación promedio para determinar un veredicto como benigno no debe tomar más de 1 minuto. El tiempo de emulación promedio para determinar un veredicto de un malware sospechoso como malware no debe tomar más de 3 minutos		
1.088			La solución de emulación de amenazas debe permitir Restricciones Geográficas, las cuales permiten que las emulaciones sean restringidas a Países en específico.		
1.089			La solución debe proveer la habilidad de incrementar la seguridad compartiendo automáticamente la información de nuevos ataques con otros Gateways utilizando la actualización de firmas entre otros		
1.090			El motor de emulación debe exceder un 90% de captura en las pruebas de Virus Totales donde los pdf´s y exe´s son modificados con encabezados ¨no usados¨ para demostrar la capacidad de la solución para detectar malware nuevo y desconocido. La solución debe detectar tráfico C&C de acuerdo la reputación dinámica de los ip/url		
1.091			La Solución debe ser capaz de emular y extraer archivos embebidos en documentos. Debe ser capaz de escanear documentos que contengan URLs		
1.092			La solución debe monitorear las actividades sospechosas en:		

1.093			Llamadas a APIs, Cambios en archivos del Sistema, Registro del Sistema, Conexiones de redes, Procesos del Sistema, Creación y borrado de archivos, Modificaciones de Archivos, Inyección de código al Kernel, Detección de intentos de escalamiento de privilegios, Modificaciones al Kernel (Cambios de memoria realizados por el código del Kernel, no el hecho de que se cargue un driver, esto esta cubierto por el elemento anterior), Comportamiento del código del Kernel, monitoreo de las actividades de código que no sea modalidad de usuario. Interacción física directa con el CPU, Detección de Bypass del Control de Acceso de Usuario.		
1.094			La solución debe poseer capacidades de anti-evasión detectando la ejecución del Sandbox. Debe ser resiliente a casos donde el código shell o el malware puede no ejecutarse si detectan la existencia de un ambiente virtual (Hipervisor propietario). Debe ser resiliente a delays implementados en las etapas del código shell o el malware. Debe ser resiliente a casos donde el código shell o el malware solo se ejecute luego de un reinicio o apagado del end point.		
1.095			La solución debe emular actividades de usuarios reales tales como clicks del ratón, uso del teclado, etc. Debe ser capaz de identificar íconos que son similares a documentos de aplicaciones populares. Debe proteger contra evasión dentro de archivos flash (swf)		
1.096			La solución debe ofrecer la funcionalidad de poder ser manejada de forma centralizada. Luego de la detección de archivos maliciosos, se debe generar un reporte detallado para cada uno de los archivos maliciosos. El reporte detallado debe incluir capturas de pantallas, líneas de tiempo, las modificaciones o creaciones clave en el registry, la creación de archivos y/o procesos, y la actividad de red detectada		
1.097			La solución debe eliminar las amenazas y remover el contenido explotable, incluyendo el contenido activo y los objetos embebidos. Debe ser capaz de reconstruir los archivos con los elementos seguros conocidos. Debe tener la capacidad de convertir los archivos reconstruidos a formato PDF. Debe mantener la flexibilidad de mantener el formato original del archivo y especificar el tipo de contenido que será removido.		
1.098			La solución de seguridad de Anti-Spam y Email debe ser agnóstica al lenguaje y al contenido. Debe poseer clasificación y protección en tiempo real basados en la detección de brotes de spam que están basados en patrones y no en contenido. Debe incluir el bloqueo de IPs basados en reputación desde un servicio online para evitar falsos positivos		

1.099			Debe incluir mecanismos de protección de Hora Cero para nuevos virus propagados a través de email y spam sin depender solamente en inspección de contenido o heurística		
1.100			Para las funcionalidades de Ipsec VPNs debe soportar CA internos y externos de terceros. Debe soportar criptografía 3DES y AES-256 para IKE fase 1 y IIIKEv2 , Suite-B-GCM-128 y Suite B-GCM-256 para fase II.		
1.101			Debe soportar por lo menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20. Debe soportar integridad de Data con md5, sha1SHA-256, SHA-384 y AES-XCBC		
1.102			La solución debe soportar VPN sitio a sitio en las siguientes topologías: Full Mesh (all to all), Star (Oficinas remotas con sitio principal), Hub and Spoke (Sitio Remoto a través del Sitio Central con otro Sitio Remoto). Debe soportar la configuración de los VPNs mediante un GUI que permita la adición de objetos a las comunidades de VPNs mediante drag and drop.		
1.103			Debe soportar SSL VPN clientless para acceso remoto. Deben soportar VPNs L2TP incluyendo los clientes para Iphones.		
1.104			Debe permitir que el administrador aplique las reglas de seguridad para controlar el tráfico dentro de los VPNs. Debe soportar VPNs basados en dominios, y rutas usando protocolos de ruteo dinámico y VTIs. Debe incluir la habilidad de establecer VPNs dentro de gateways con IPs dinámicas públicas y compresión IP para VPNs cliente a sitio y sitio a sitio.		
1.105			La aplicación de manejo de seguridad debe soportar cuentas de administradores basadas en roles, ejemplo, un rol solo para establecimiento de las políticas de firewall o un rol solo para visualización. Debe incluir canales de comunicación seguros basados en encripción de Certificados para todas las soluciones de diferentes fabricantes que pertenezcan a un dominio de gerencia.		
1.106			La solución debe incluir una Autoridad de Certificados Interna, x509 CA que pueda generar Certificados a gateways y usuarios para permitir un mecanismo eficiente de autenticación en los VPNs. Debe incluir la capacidad de usar CA s externos que soporten estándares PKCS#12, CAPI o ENTRUST		
1.107			Todas las aplicaciones de seguridad en este grupo deben ser capaces de ser manejadas desde una consola central. La solución de gerencia debe proveer un conteo de los hits a las reglas de seguridad en las políticas de seguridad. Debe incluir opciones de búsqueda que permitan investigar cual objeto de red contiene una dirección IP específica o una parte de ella.		

1.108			Debe incluir la opción de segmentar la base de reglas utilizando etiquetas o títulos de secciones para mejor organización de las políticas. Debe proveer la opción de salvar la política completa o una parte específica de la misma. Debe poseer mecanismos de verificación de políticas de seguridad previo a la instalación de las mismas. Debe poseer mecanismos de control de revisión de las políticas de seguridad.		
1.109			La solución debe proveer las opciones de añadir alta disponibilidad a la gerencia de seguridad, usando un servidor de gerencia standby que se sincroniza automáticamente con el servidor activo sin la necesidad de dispositivos externos de almacenamiento. Esta funcionalidad debe ser incluida en las propuestas de la licitación.		
1.110			La solución de seguridad debe incluir un mapa comprensivo de todos los objetos de redes y sus conexiones que pueda ser exportado a Microsoft Visio o a un archivo de imágenes.		
1.111			Debe incluir la habilidad de distribuir y aplicar de forma centralizada nuevas versiones de software a los diferentes gateways de seguridad. Debe incluir una herramienta de manejo de las licencias de los diferentes gateways de seguridad que debe ser controlada por la estación de gerencia. Debe tener la capacidad de manejo de multi dominios y soportar la funcionalidad de políticas de seguridad globales a través de los dominios.		
1.112			El interfase gráfico de la herramienta de gerencia debe tener la habilidad de poder excluir direcciones IP de la definición de firmas de la solución de IPS. Debe tener la capacidad de excluir direcciones IP de los logs de IPS cuando se detectan como falsos positivos. Debe ser capaz de alcanzar las definiciones de firmas de IPS desde los logs de IPS.		
1.113			El licitante debe proveer los detalles de sus mecanismos de actualización y de su habilidad para manejar ataques de día cero a través de todas las soluciones de prevención de amenazas incluyendo IPS, Control de Aplicaciones, Filtrado de URL, Anti BOT y anti Virus. Debe proveer los detalles de la categorización de los URLs bajo las circunstancias de que ese website haya sido comprometido y este distribuyendo malware		
1.114			El mecanismo de logging central debe ser parte del sistema de administración, los administradores deben tener la capacidad de instalar servidores de almacenamiento de Logs adicionales.		

1.115			La operación de logs debe proveer la opción de operar en el servidor de gerencia o en servidores dedicados. Debe ser capaz de operar en servidores X86 abiertos. Se debe entregar la lista de compatibilidad. La solución debe tener la habilidad de almacenar todos los logs para todas las reglas de seguridad. El buscador de logs debe tener la capacidad de realizar búsquedas indexadas.		
1.116			La solución debe tener la capacidad de hacer logs a todas las aplicaciones integradas en esta solución, incluyendo IPS, Aplication Control, URL Filtering, Antivirus, AntiBOT, User Identity.		
1.117			La solución debe incluir un mecanismo de captura automática de paquetes para los eventos de IPS de forma tal que se puedan realizar mejores análisis forénsicos. Debe proveer diferentes logs para regular las actividades de los usuarios y los relacionados a la gerencia.		
1.118			La solución debe proveer para cada ocurrencia de un hit de reglas de seguridad las siguientes opciones: LOG, alerta, trap SNMP, email o la ejecución de un script definido por el usuario. Los LOGs debe tener un canal seguro de comunicaciones para la transferencia de los mismos para evitar escuchas, esta solución debe estar autenticada y encriptada. Los logs deben ser transferidos de manera segura entre el gateway, la gerencia, los servidores dedicados de LOGs y las consolas de visualización en las estaciones de los administradores		
1.119			La solución debe incluir la opción de bloquear dinámicamente una conexión activa desde el interfase gráfico del LOG sin necesidad de modificar las bases de reglas. Debe ser capaz de exportar logs en formato de bases de datos. Debe soportar el cambio automático del archivo de LOGs basado en tiempos preestablecidos o en el tamaño de los archivos		
1.120			Debe soportar el manejo de excepciones a los enforzamientos IPS desde el record de LOG. Debe ser capaz de asociar un nombre de usuario y un nombre de máquina a cada record de LOG.		
1.121			La herramienta de manejo gráfica debe ser capaz de monitorear fácilmente el estatus de los gateways. Esta herramienta debe proveer información del sistema para cada gateway, incluyendo: uso de memoria, CPU, particiones de discos y espacio restante. Debe proveer el status de cada componente del gateway tales como firewall, vpn, clúster, antivirus, etc. Debe incluir el estatus de todos los túneles de VPNs, sitio a sitio y cliente a sitio.		

1.122			La solución debe permitir la definición de umbrales y de las acciones a realizar cuando los mismos son alcanzados en los gateways. Las acciones deben incluir: LOGs, Alertas, traps SNMP, email y la ejecución de un script definido por el usuario. Debe incluir gráficos pre configurados para monitorear la evolución en el tiempo del tráfico y de los contadores del sistema: reglas de seguridad máximas, usuarios P2P, túneles VPNs, tráfico de red y otras informaciones útiles. Debe proveer la funcionalidad de generar nuevos gráficos personalizados usando diferentes tipos de tablas.		
1.123			La solución debe proveer la capacidad de grabar las vistas de tráfico y de sistemas para visualización futura en cualquier momento. Debe ser capaz de reconocer el mal funcionamiento y los problemas de conectividad entre dos puntos conectados a través de un VPN, y crear logs y realizar alertas cuando un túnel VPN está abajo		
1.124			La funcionalidad de correlación de eventos debe estar integrada totalmente en la aplicación de gerencia. Debe incluir herramientas para correlacionar eventos de todas las funcionalidades del gateway y de dispositivos y soluciones de terceros. Debe permitir la creación de filtros basados en cualquier característica de evento tales como aplicaciones de seguridad, direcciones IP origen y destino, servicio, tipo de evento, severidad, nombre del ataque, país de origen y destino, etc. Debe tener un mecanismo de asignación de estos filtros a diferentes gráficos de línea que puedan ser actualizados a intervalos regulares mostrando todos los eventos correspondientes a ese filtro, esto le permite al operador enfocarse en los eventos más importantes.		
1.125			La funcionalidad de correlación de eventos debe suministrar una vista gráfica de los eventos basados en tiempo. Debe mostrar la distribución de eventos por países en un mapa. Debe permitir al administrador a agrupar los eventos basados en cualquiera de sus características incluyendo niveles de anidamiento y su exportación en formato PDF.		
1.126			La funcionalidad debe incluir la opción de búsqueda dentro de la lista de eventos, y el drill down en los detalles para la investigación y análisis forénsico. Se debe incluir la funcionalidad de la creación de tablas gráficas con las características de los eventos.		
1.127			La solución debe ser capaz de detectar ataques de Negación de Servicios correlacionando eventos de todas las fuentes. Debe detectar un login de administrador en horas irregulares. Debe detectar ataques de adivinación de credenciales. La solución debe reportar sobre todas las instalaciones de políticas de seguridad.		

1.128			La solución debe incluir reportes predefinidos por hora, día, semana y mes incluyendo por lo menos los Eventos, Fuentes, Destinos, Servicios, Fuentes máximos, Fuentes máximas y sus eventos máximos, Destinos máximos y sus eventos máximos y los servicios máximos y sus eventos máximos. La herramienta de reportes debe permitir la aplicación de por lo menos 25 filtros que permitan personalizar los reportes predefinidos de acuerdo a las necesidades de los administradores		
1.129			La herramienta de reportes debe soportar la calendarización automática de los reportes para la información que debe ser extraída de forma regular (día, semana, mes). La solución debe permitir al administrador definir la fecha y hora en que los reportes comienzan a generarse. Debe soportar formatos de reporte HTML, CSV y MHT. Debe soportar la distribución automáticas por email, la subida a servidores FTP/WEB y scripts personalizados de distribución de los mismos.		
1.130			El sistema de reportes debe proveer información consolidada sobre: El volumen de conexiones que fueron bloqueadas por reglas de seguridad. Las fuentes máximas de las conexiones bloqueadas, su destino y servicios. Reglas máximas usadas por las políticas de seguridad por los puntos de enforzamiento (perímetro). Servicios de redes máximos. Actividad WEB por usuarios detallando los sitios más visitados y los mayores usuarios. Servicios máximos que crearon la mayor carga para el tráfico encriptado. Usuarios máximos de VPNs que realizan las conexiones de mayor duración.		
1.131			La solución debe incluir un Portal de Gerencia con acceso basado en browser para visualizar en modo solo lectura las políticas de seguridad, manejar los logs de los firewalls y usuarios, proveyendo acceso a los gerentes y auditores sin la necesidad de usar la aplicación de gerencia. Esta solución debe incluir soporte SSL y puertos configurables.		
1.132			La solución de Seguridad debe incluir una aplicación completamente integrada de Data Loss Prevention (DLT) que debe ser manejada de manera centralizada con las otras aplicaciones de seguridad de esta suite.		
1.133			La aplicación de DLT debe tener mecanismos para el manejo de auto-incidentes de usuarios finales. Debe tener un mínimo de 500 tipos de data predefinidos. Debe poseer un lenguaje de creación de scripts para poder definir tipos de data relevantes a cada organización. Debe alertar al dueño del tipo de data cuando ocurre un incidente. Debe cubrir tipos de transporte SMTP, HTTP/HTTPS y protocolos FTP y TCP		

1.134			La solución integrada de seguridad debe ofrecer una funcionalidad completa para asegurar los dispositivos móviles. Debe soportar tanto los dispositivos gerenciados como los no gerenciados tales como los BYOD.		
1.135			La solución debe incluir todo el hardware, software, y licencias necesarias para poder manejar el siguiente dimensionamiento: Manejo de un Ancho de Banda Agregada de Acceso a Internet de por lo menos 500 Gbps y capacidad de crecimiento para por lo menos 1 Gbps. Capacidad de manejo de mínimo de 8 conexiones independientes a distintos proveedores de servicios. Configurada y licenciada para manejar un mínimo de 1200 end points, 1200 buzones de correo y 400 máquinas virtuales de servidores que pueden correr sistemas operativos Windows, Linux o Solaris		
1.136			La solución debe tener un mínimo de 100 reglas de seguridad pre configuradas		
1.137			La solución integrada debe ofrecer las siguiente soluciones de seguridad para todo este dimensionamiento : Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación de Amenazas y Extracción de Amenazas, VPNs IPsec, Data Loss Prevention		
1.138			Las soluciones de Hardware deben ser ofertadas en clusters de alta disponibilidad con fuentes de poder y abanicos redundantes.		
1.139			La solución debe ser capaz de trabajar de forma coordinada e integrada con la solución de seguridad de Sandboxing		
2.000		***Expansión de la Solución de Web Application Firewall, Application Delivery, Balanceador y Protección de DDOS para Centro de Recuperación de Operaciones***		***CUMPLE***	***NO CUMPLE***
2.001	1	***Expansión de la Solución de Web Application Firewall, Application Delivery, Balanceador y Protección de DDOS para Centro de Recuperación de Operaciones***	CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO		

2.002			Los equipos ofertados debe ser una plataforma de hardware de propósito específico denominado "appliance".		
2.003			El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.		
2.004			Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado.		
2.005			Se debe ofrecer dos (2) equipos en Alta disponibilidad funcionando en configuración de Par Activo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.		
2.006			Cada equipo debe cumplir con las siguientes características:		
2.007			La solución debe soportar un Throughput en L4 de al menos 20 Gbps La solución debe soportar un Throughput en L7 de al menos 20 Gbps		
2.008			La solución debe soportar al menos 28 Millones de conexiones simultáneas La solución debe soportar al menos 250.000 conexiones por segundo en L4		
2.009			La solución debe soportar al menos 1 Millón de HTTP Requests por Segundo Cada equipo debe contar con al menos las siguientes Interfaces de red: Al menos 8 puertos SFP a 1Gbps		
2.010			Al menos 4 puertos SFP+ a 10 Gbps Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap) y certificadas 80 Plus Platinum" para eficiencia energética.		
2.011			Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.		

2.012			Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.		
2.013			Cada equipo debe incluir 32 Gb de Memoria RAM mínimo		
2.014			Cada equipo debe incluir mínimo dos Disco duros de 500Gb en RAID 1		
2.015			Debe soportar clúster Activo/Activo y Activo/Pasivo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).		
2.016			La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda		
2.017			Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.		
2.018			Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.		
2.019			La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.		
2.020			Los equipos deben tener hardware acelerador FPGA personalizables y programables para varias funciones como protección DDoS, protocolos SDN y manejo de trafico UDP		
2.021			FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO		
2.022			La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web (protocolos de capas superiores)		
2.023			La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.		

2.024			La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.		
2.025			La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.		
2.026			Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones		
2.027			La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting:		
2.028			Round Robin Proporcional (Ratio)		
2.029			Proporcional dinámico Respuesta más rápida		
2.030			Conexiones mínimas Menor número de sesiones		
2.031			Tendencia de menor cantidad de conexiones Tendencia de desempeño		
2.032			Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM		
2.033			El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)		
2.034			El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.		

2.035			La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica		
2.036			La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:		
2.037			Ping. Chequeo a nivel de TCP y UDP a puertos específicos		
2.038			Monitoreo http y https Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.		
2.039			Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. Ejecución de scripts para determinar la respuesta emulando un cliente.		
2.040			Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma		

2.041			Monitoreo de aplicaciones de mercado: ○ LDAP ○ FTP ○ SMTP ○ IMAP/POP3 ○ Oracle ○ MSSQL ○ MySQL ○ RADIUS ○ SIP ○ Protocolo SASP ○ SOAP ○ WMI ○ SNMP Debe poder realizar todos estos métodos de persistencia de las conexiones: Dirección IP origen		
2.042			Dirección IP destino Cookies		
2.043			Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia		
2.044			Sesiones SSL Microsoft Remote Desktop		
2.045			Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.		
2.046			Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.		
2.047			El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.		

2.048			Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:		
2.049			Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados. Soporte de REST API Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts. Debe soportar el protocolo TDS para balanceo de MSSQL Debe soportar el protocolo NetFlow (v5 El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script. La solución debe permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código. El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3 Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el		

			mismo equipo sin necesidad de acceso a Internet (offline). Incluir el soporte de Aceleración SSL usando Hardware Dedicado FUNCIONES DE SEGURIDAD GENERALES Cada equipo debe soportar seguridad SSL con las siguientes características:		
2.050			Incluir mínimo 10.000 Transacciones por segundo SSL (RSA 2K Keys) Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits		
2.051			Soportar al menos 10 Gbps SSL Bulk Encryption (Thoughput SSL) Incluir mínimo 6.500 Transacciones por segundo SSL (ECDSA P-256)		
2.052			La solución debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener la sesión SSL		
2.053			El Stack TLS del equipo debe soportar las siguientes funcionalidades/características		
2.054			Session ID Session Ticket		
2.055			OCSP Stapling (on line certificate status protocol) Dynamic Record Sizing		
2.056			ALPN (Application Layer Protocol Negotiation) Forward Secrecy		
2.057			La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)		
2.058			Debe soportar algoritmos de cifrado Camellia		
2.059			El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall)		
2.060			El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall		
2.061			Firmado criptográfico de cookies para verificar su integridad.		

2.062			Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto) Luna.		
2.063			La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.		
2.064			Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.		
2.065			Debe soportar HSTS (HTTP Strict Transport Security)		
2.066			Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.		
2.067			Scanners Exploits Windows		
2.068			Denial of Service Proxies de Phishing		
2.069			Botnets Proxies anónimos		
2.070			FUNCIONES DE ACELERACIÓN DE TRÁFICO		
2.071			La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:		
2.072			Memoria cache. Compresión tráfico HTTP		
2.073			Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores		

2.074			El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.		
2.075			Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 6 Gbps o superior usando aceleración por Hardware dedicado, no la CPU de propósito general.		
2.076			Debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.		
2.077			Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos		
2.078			Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP		
2.079			DNS Y BALANCEO A DE ENLACES DE INTERNET		
2.080			La solución debe soportar el permitir alta disponibilidad de aplicaciones distribuidas en 2 o más Centro de Datoss, sin importar la ubicación geográfica.		
2.081			Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.		
2.082			Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.		
2.083			Para el balanceo global (DNS), debe permitir los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting:		
2.084			Round Robin Global Availability		
2.085			Geolocalización Capacidad del Servicio		
2.086			Least Connections Packets Per Second		
2.087			Round Trip Time Drop Packet		

2.088			Hops Packet Completion Rate		
2.089			User-defined QoS Proporcional (Ratio)		
2.090			Kilobytes Per Second Regreso al DNS		
2.091			Persistencia estática Puntuación del Servicio		
2.092			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo Centro de Datos por el transcurso de su sesión.		
2.093			Permitir Balanceo de cargas ente Centro de Datoss de acuerdo a la ubicación geográfica		
2.094			Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico basado en requerimientos particulares de la infraestructura		
2.095			Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.		
2.096			Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.		
2.097			Debe permitir realizar balanceo de servidores DNS.		
2.098			Debe soportar el protocolo DNSSEC		
2.099			Debe incluir herramienta de administración grafica para el manejo de zonas DNS		
2.100			Debe soportar registros AAAA para IPv6		
2.101			Debe soportar traducción entre DNS IPv4 y DNS IPv6		
2.102			La solución debe soportar 480.000 respuestas DNS por segundo.		
2.103			La solución debe permitir balanceo de enlaces de internet, sin restringir el numero de enlaces y sin importar el proveedor de estos.		

2.104			Debe proveer balanceo de tráfico saliente entre múltiples ISP y detectar el fallo de alguno de ellos para enrutar automáticamente el tráfico hacia los demás ISP.		
2.105			Debe proveer balanceo de trafico entrante, basado en DNS y responder autoritativamente a queries DNS tipo A		
2.106			Debe permitir monitoreo de los enlaces y detectar fallos en ellos.		
2.107			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo ISP por el transcurso de su sesión		
2.108			FUNCIONES DE FIREWALL Y PROTECCION DDOS		
2.109			Debe incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables		
2.110			La solución de DDoS debe contar con un sistema de protección basado en comportamiento (Behavioral) que permita la creación de firmas o vectores de ataque de manera dinámica.		
2.111			La solución debe proteger contra ataques de denegación de servicio tanto en una topología en línea (inline deployment) como en una topología fuera de línea (TAP mode)		
2.112			Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks		
2.113			Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP		
2.114			Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.		
2.115			Debe permitir la creación de reglas globales.		
2.116			Debe tener la opción de funcionar como un firewall statefull full-proxy y ser certificado por ICSA Labs como Network Firewall		
2.117			Debe permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas		
2.118			Entre intervalos de tiempo		
2.119			Hasta una fecha especifica		
2.120			Después de una fecha específica.		
2.121			Debe permitir la creación de listas blancas (White lists) de direcciones IP		
2.122			Debe permitir la configuración de túnel IPSEC Site-to-Site		

2.123			Debe incluir funcionalidad de application delivery controller o integrarse con dispositivos de Application Delivery		
2.124			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo		
2.125			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo		
2.126			Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.		
2.127			Debe funcionar como un Proxy SSH para control de conexiones entre diferentes redes con el fin de dar visibilidad a las sesiones SSH y controlar las mismas		
2.128			Debe soportar Port Misuse, evitando que servicios pasando a través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).		
2.129			Debe soportar RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.		
2.130			Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT		
2.131			ESTÁNDARES DE RED		
2.132			Soporte VLAN 802.1q, Vlan tagging		
2.133			Soporte de 802.3ad para definición de múltiples troncales		
2.134			Soporte de NAT, SNAT		
2.135			Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.		
2.136			Soporte de Rate Shapping.		
2.137			Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.		

2.138			Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.		
2.139			Debe soportar el protocol de OVSDB (Open vSwitch Database) para crear túneles VXLAN usando un controlador SDN		
2.140			Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS		
2.141			ADMINISTRACIÓN DEL SISTEMA		
2.142			La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)		
2.143			La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.		
2.144			La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.		
2.145			La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.		
2.146			La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales		
2.147			La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:		
2.148			Protocolo SysLog Notificación vía SMTP		
2.149			SNMP versión.2.0 o superior. El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico. El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque. La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real		

			Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos. Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.		
3.000		***Expansión de la Solución de Seguridad para la Estructura Virtual***		***CUMPLE***	***NO CUMPLE***
3.001	***1***	***Expansión de la Solución de Seguridad para la Estructura Virtual, integrada con los Gateways de Manejo y Control de Seguridad Integrada redundantes. La solución actual está basada en equipos Checkpoint.***	Se requiere una expansión de la solución de seguridad integrada de los Gateways de Manejo y Control de Seguridad Integrada redundantes actuales, para el manejo de la Infraestructura Virtual del Ministerio. Esta Estructura virtual está basada en VMWare. La solución ofertada debe incluir todos los componentes necesarios, los servicios de configuración, implementación y puesta a punto de misma y Soporte Técnico y Mantenimiento de la misma por parte del fabricante por un período de 3 años con tiempo de respuesta NBD 8X5. La solución debe cumplir mínimo con los siguientes requerimientos técnicos:		
3.002			La solución debe soportar la implementación con el Hipervisor de vCNS		
3.003			La solución debe soportar la implementación con el Hipervisor de NSX		
3.004			La solución debe soportar la importación de objetos virtuales directamente desde el Vcenter hacia las políticas de seguridad sin ninguna configuración manual en el vCenter y/o el NSX		
3.005			La solución debe soportar la importación de Grupos de Seguridad directamente desde NSX hacia las políticas de seguridad		

3.006			La solución debe permitir las conexión e importación de objetos virtuales desde mas de un NSX/vCenter		
3.007			La solución debe ser capaz de manejar objetos virtuales in las políticas globales de seguridad de los dispositivos norte-sur incluso si redirecionar el tráfico a traves del NSX		
3.008			La solución debe permitir la implementación de múltiples instancias de pasarelas de seguridad en el mismo host ESXi		
3.009			La solución debe ser certificada y compatible con VMWare		
3.010			La solución debe permitir las opciones de fallo-abierto/fallo-cerrado para cada instancia en caso de que no haya conectividad con Vcenter o NSX		
3.011			La solución debe permitir la instalación de políticas de seguridad en las instancias virtuales antes de que el tráfico sea redireccionado en el NSX		
3.012			La solución debe permitir la orquestación de las políticas de seguridad utilizando reglas de aprovisionamiento de auto-servicio		
3.013			La solución debe tener creados los flujos de reglas de aprovisionamiento de las políticas de seguridad		
3.014			La solución debe permitir que los administradores y orquestadores del data center utilicen automatización segura solo para políticas de seguridad específicas		
3.015			La solución debe ofrecer desde el principio las capacidades de etiquetamiento de Máquinas Virtuales que permitan la actualización del NSX con los estados de seguridad de las acciones de automatización		
3.016			La solución debe ofrecer el manejo unificado de las pasarelas de centro de datos tanto virtuales como físicas		
3.017			La solución debe permitir la visualización de los nombre de los objetos en los logs de seguridad en adición a las direcciones IP de las Máquinas Virtuales		
3.018			La solución debe tener sub-políticas dedicadas por micro-segmentos con privilegios de administración granulares		
3.019			La solución debe soportar permisos dedicados para funciones y aplicaciones de niveles de políticas de seguridad específicos (Aplicaciones, Prevención de Amenazas, etc)		

3.020			La solución debe ser capaz de tener visibilidad en las políticas de seguridad de las Máquinas Virtuales y los parametros de las mismas (IP, localización en el Centro de Datos, Sistema Operativo, etc)		
3.021			Las redes virtuales deberán aprovisionar y administrar de forma programática, independientemente del hardware subyacente		
3.022			Deberá permitir reproducir el modelo de red completo en Software, permitiendo la creación y aprovisionamiento de cualquier topología de red, desde redes simples hasta redes complejas de múltiples niveles		
3.023			Deberá permitir reducir el tiempo de aprovisionamiento de redes, asi como permitir mejoras operacionales por medio de la automatización.		
3.024			Deberá ser ompatible con overlays de redes basadas en LAN virtual extensible (Virtual eXtensible LAN, VXLAN).		
3.025			Deberá permitir enrutamiento dinámico entre redes virtuales realizado de manera distribuida en el kernel del hipervisor, enrutamiento con escalabilidad horizontal y con conmutación de recuperación activo-activo, mediante enrutadores físicos.		
3.026			Deberá soportar enrutamiento dinámico por medio de los protocolos BGP y OSPF así como enrutamiento estático.		
3.027			Deberá tener la capacidad de conexión de VXLAN a redes físicas soportadas por VLAN para conexiones a cargas de trabajo físicas		
3.028			Deberá ofrecer una Interface para el desarrollo de aplicaciones (API) tipo RESTful para la integración de cualquier plataforma de administración de nube o automatización.		
3.029			Deberá incorporar las siguientes capacidades que soporten la operación de la plataforma: Interfaz de línea de Comandos Analizador de Trazas y flujos Analizador de puerto del switch (SPAN) Exportación de Flujos basado en IPFIX Integración con la herramienta de operaciones VMware vRealize Operations Integración con la herramienta vRealize Log Insight		

3.030			La plataforma deberá ofrecer integración nativa con vRealize Automation y OpenStack		
3.031			Automatización: Deberá permitir crear redes basadas en software, abordando los desafíos en el aprovisionamiento prolongado de redes, errores de configuración y procesos costosos, todo esto mediante el apovechamiento de la automatización		
3.032			Deberá ofrecerse una plataforma para la seguridad y virtualización para ambientes VMware vSphere que funcione como Hipervisor de red		
3.033			La plataforma deberá incorporar las siguientes funciones de red, incorporados directamente en el hipervisor ESXi y distribuídas en el entorno vSphere : Enrutamiento Conmutación de datos Protección de Firewall		
3.034			Deberá suministrar micro-segmentación y seguridad granular y detallada para la carga de trabajo individual.		
3.035			Deberá soportar protección de firewall distribuido e incorporado en el kernel del hipervisor para hasta 20 Gbps de capacidad de firewall por host hipervisor. La protección deberá ser sin pérdida del estado de las sesiones, lo anterior conocido como Stateful Firewall		
3.036			En adición al firewall incorporado en el hipervisor, deberá soportar un Firewall para comunicacones Norte-Sur.		
3.037			Deberá ofrecer capacidades de VPN tipo Sitio a Sitio		
3.038			Deberá ofrecer capacidades de VPN de tipo Acceso Remoto		
3.039			Las capacidades de micro-segmentación permitirán crear grupos de seguridad dinámicos y asociados con base a factores que van más allá de la dirección IP y MAC; dichos grupos deberán aprovechar los objetos y etiquedas de VMware vCenter, tipo de sistema operativo, información sobre aplicaciones de capa 7.		
3.040			Seguridad: Deberá permitir dividir de manera lógica el centro de datos en distintos segmentos de seguridad hasta el nivel de la carga de trabajo individual, con independencia de la subred o VLAN, permitiendo definir políticas y controles de seguridad según los grupos de seguridad dinámicos, evitando el movimiento lateral dentro del Centro de Datos.		

3.041			Deberá incorporar los siguientes elementos y servicios de red lógicos como parte de la misma plataforma: Switches Lógicos** Enrutamiento** Protección de Firewall Balaneo de Carga Red Privada Virtual (VPN) Calidad de Servicio (QoS) Monitoreo		
3.042			Deberá permitir la movilidad de cargas de trabajo independiente de la topología de red física entre centros de datos y dentro de ellos.		
3.043			Deberá soportar servicios de seguridad y de red avanzados a través de integraciones con terceros		
3.044			Deberá permitir extensiones de overlay de la capa 2 lógica en una estructura de conexión enrutada (capa 3, C3) dentro de los límites del centro de datos y entre ellos.		
3.045			El Firewall distribuido e incorporado en el kernel del hipervsor deberá ser compatible con Active Directory.		
3.046			Deberá incorporar un servicio de Balanceo de Cargas de Capa 4 a Capa 7 (modelo OSI) con capacidad de descargar y transferencia de tráfico cifrado SSL.		
3.047			El servicio de Balanceo de Cargas deberá tener la capacidad de comprobar el estado del servidior		
3.048			El Servicio de Balanceo de Cargas deberá tener la capacidad de aplicar reglas de aplicación que permitan la programación y la manipulación del tráfico.		
3.049			La plataforma deberá permitir integrarse con funciones del plano de control, plano de datos y administración con socios de terceros en distintas variedades como Firewalls de próxima generación, Sistemas de Detección de Intrusos (IDS), Sistemas de Prevención de Intrusos (IPS), Antivirus sin agentes, Controladores de suministro de aplicaciones, Conmutaciones, Operaciones y Visibilidad.		
3.050			Deberá ofrecer la capacidad de extender la seguridad y las redes a través de los límites del centro de datos, con independencia de la topología física subyacente, lo que permitirá obtener capacidades como recuperación ante desastres y centros de datos Activo-Activo.		

3.051			Continuidad de las aplicaciones: Deberá permitir replicar fácilmente entornos de aplicaciones completos en centros de datos remotos para la recuperación ante desastres, lo anterior mediante la separación de las redes del hardware subyacente, sin afectar el funcionamiento de las aplicaciones y sin tocar la red física.		
3.052			Debe incorporar herramientas nativa para la gestión de reglas y monitoreo de terminales, para obtener una visualización integral de flujos de tráfico de red hasta la capa 7 del modelo OSI, permitiendo la identificación de terminales en el centro de datos y entre centros de datos y respondan mediante la creación de reglas de seguridad adecuadas		
3.053			Se deben incluir y describir explícitamente 5 cupos de formación profesional oficiales, válidos para los esquemas de Certificación Profesional y avanzada de cada uno de los fabricantes, de cada una de las soluciones ofertadas. Estos cursos deben ofrecerse en la Ciudad de Santo Domingo y deben incluir toda la documentación y material de soporte de los mismos. En caso de no poder ser ofrecidos en la Ciudad de Santo Domingo, se deben incluir los costos de viáticos para los mismos.		

3.5 Fase de Homologación

Una vez concluida la recepción de los **"Sobres A",** se procederá a la valoración de las muestras, si aplica, de acuerdo a las especificaciones requeridas en las Fichas Técnicas y a la ponderación de la documentación solicitada al efecto, bajo la modalidad **"CUMPLE/ NO CUMPLE".**

Para que un Bien pueda ser considerado **CONFORME**, deberá cumplir con todas y cada una de las características contenidas en las referidas Fichas Técnicas. Es decir que, el no cumplimiento en una de las especificaciones, implica la descalificación de la Oferta y la declaración de **NO CONFORME** del Bien ofertado.

Los Peritos levantarán un informe donde se indicará el cumplimiento o no de las Especificaciones Técnicas de cada uno de los Bienes y Servicios conexos ofertados, bajo el criterio de **CONFORME/ NO CONFORME**. En el caso de no cumplimiento indicará, de forma individualizada las razones.

Los Peritos emitirán su informe al Comité de Compras y Contrataciones sobre los resultados de la evaluación de las Propuestas Técnicas "Sobre A", a los fines de la recomendación final.

3.6 Apertura de los "Sobres B", Contentivos de Propuestas Económicas

El Comité de Compras y Contrataciones, dará inicio al Acto de Apertura y lectura de las Ofertas Económicas, **"Sobre B",** conforme a la hora y en el lugar indicado.

Sólo se abrirán las Ofertas Económicas de los Oferentes/Proponentes que hayan resultado habilitados en la primera etapa del proceso. Son éstos aquellos que una vez finalizada la evaluación de las Ofertas Técnicas, cumplan con los criterios señalados en la sección Criterios de evaluación. Las demás serán devueltas sin abrir. De igual modo, solo se dará lectura a los renglones que hayan resultado CONFORME en el proceso de evaluación de las Ofertas Técnicas.

A la hora fijada en el Cronograma del Procedimiento de Excepción de Proveedor Único, el Consultor Jurídico de la institución, en su calidad de Asesor Legal del Comité de Compras y Contrataciones, hará entrega formal al Notario Público actuante, en presencia de los Oferentes, de las Propuestas Económicas, **"Sobre B",** que se mantenían bajo su custodia, para dar inicio al procedimiento de apertura y lectura de las mismas.

En acto público y en presencia de todos los interesados el Notario actuante procederá a la apertura y lectura de las Ofertas Económicas, certificando su contenido, rubricando y sellando cada página contenida en el **"Sobre B".**

Las observaciones referentes a la Oferta que se esté leyendo, deberán realizarse en ese mismo instante, levantando la mano para tomar la palabra. El o los Notarios actuantes procederán a hacer constar todas las incidencias que se vayan presentando durante la lectura.
Finalizada la lectura de las Ofertas, el o los Notarios actuantes procederán a invitar a los Representantes Legales de los Oferentes/Proponentes a hacer conocer sus observaciones; en caso de conformidad, se procederá a la clausura del acto.

No se permitirá a ninguno de los presentes exteriorizar opiniones de tipo personal o calificativos peyorativos en contra de cualquiera de los Oferentes participantes.

El Oferente/Proponente o su representante que durante el proceso del Procedimiento de Excepción de Proveedor Único tome la palabra sin ser autorizado o exteriorice opiniones despectivas sobre algún producto o compañía, será sancionado con el retiro de su presencia del salón, con la finalidad de mantener el orden.

En caso de discrepancia entre la Oferta presentada en el formulario correspondiente, **(SNCC.F.033)**, debidamente recibido por el Notario Público actuante y la lectura de la misma, prevalecerá el documento escrito.

El o los Notarios Públicos actuantes elaborarán el acta notarial correspondiente, incluyendo las observaciones realizadas al desarrollo del acto de apertura, si las hubiera, por parte de los Representantes Legales de los Oferentes/ Proponentes. El acta notarial deberá estar acompañada de una fotocopia de todas las Ofertas presentadas. Dichas actas notariales estarán disponibles para los Representantes Legales de los Oferentes/Proponentes, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.7 Confidencialidad del Proceso

Las informaciones relativas al análisis, aclaración, evaluación y comparación de las Ofertas y las recomendaciones para la Adjudicación del Contrato no podrán ser reveladas a los Licitantes ni a otra persona que no participe oficialmente en dicho proceso hasta que se haya anunciado el nombre del Adjudicatario, a excepción de que se trate del informe de evaluación del propio Licitante. Todo intento de un Oferente para influir en el procesamiento de las Ofertas o decisión de la Adjudicación por parte del Contratante podrá dar lugar al rechazo de la Oferta de ese Oferente.

3.8 Plazo de Mantenimiento de Oferta

Los Oferentes/Proponentes deberán mantener las Ofertas por el término de **treinta (30)** días hábiles contados a partir de la fecha del acto de apertura.

La Entidad Contratante, excepcionalmente podrá solicitar a los Oferentes/Proponentes una prórroga, antes del vencimiento del período de validez de sus Ofertas, con indicación del plazo. Los Oferentes/Proponentes podrán rechazar dicha solicitud, considerándose por tanto que han retirado sus Ofertas, por lo cual la Entidad Contratante procederá a efectuar la devolución de la Garantía de Seriedad de Oferta ya constituida. Aquellos que la consientan no podrán modificar sus Ofertas y deberán ampliar el plazo de la Garantía de Seriedad de Oferta oportunamente constituida.

3.9 Evaluación Oferta Económica

El Comité de Compras y Contrataciones evaluará y comparará únicamente las Ofertas que se ajustan sustancialmente al presente Pliego de Condiciones Específicas y que hayan sido evaluadas técnicamente como **CONFORME**, bajo el criterio del menor precio ofertado.

Sección IV
Adjudicación

4.1 Criterios de Adjudicación

El Comité de Compras y Contrataciones evaluará las Ofertas dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás, que regulan la actividad contractual, y comunicará por escrito al Oferente/Proponente que resulte favorecido. Al efecto, se tendrán en cuenta los factores económicos y técnicos más favorables.

La Adjudicación será decidida a favor del Oferente/Proponente cuya propuesta cumpla con los requisitos exigidos y sea calificada como la más conveniente para los intereses institucionales, teniendo en cuenta el precio, la calidad, y las demás condiciones que se establecen en el presente Pliego de Condiciones Específicas.

Si se presentase una sola Oferta, ella deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en el Pliego de Condiciones Específicas, se le considera conveniente a los intereses de la Institución.

4.2 Empate entre Oferentes

En caso de empate entre dos o más Oferentes/Proponentes, se procederá de acuerdo al siguiente procedimiento:

El Comité de Compras y Contrataciones procederá por una elección al azar, en presencia de Notario Público y de los interesados, utilizando para tales fines el procedimiento de sorteo.

4.3 Declaración de Desierto

El Comité de Compras y Contrataciones podrá declarar desierto el procedimiento, total o parcialmente, en los siguientes casos:

- Por no haberse presentado Ofertas.
- Por haberse rechazado, descalificado, o porque son inconvenientes para los intereses nacionales o institucionales todas las Ofertas o la única presentada.

En la Declaratoria de Desierto, la Entidad Contratante podrá reabrirlo dando un plazo para la presentación de Propuestas de hasta un **cincuenta por ciento (50%)** del plazo del proceso fallido.

4.4 Acuerdo de Adjudicación

El Comité de Compras y Contrataciones luego del proceso de verificación y validación del informe de recomendación de Adjudicación, conoce las incidencias y si procede, aprueban el mismo y emiten el acta contentiva de la Resolución de Adjudicación.

Ordena a la Unidad Operativa de Compras y Contrataciones la Notificación de la Adjudicación y sus anexos a todos los Oferentes participantes, conforme al procedimiento y plazo establecido en el Cronograma de Actividades del Pliego de Condiciones Específicas.

4.5 Adjudicaciones Posteriores

En caso de incumplimiento del Oferente Adjudicatario, la Entidad Contratante procederá a solicitar, mediante ***"Carta de Solicitud de Disponibilidad"***, al siguiente Oferente/Proponente que certifique si está en capacidad de suplir los renglones que le fueren indicados. Dicho Oferente/Proponente contará con un plazo de **Cuarenta y Ocho (48) horas** para responder la referida solicitud. En caso de respuesta afirmativa, El Oferente/Proponente deberá presentar la Garantía de Fiel cumplimiento de Contrato, conforme se establece en los **DDPEPU.**

.

PARTE 2
CONTRATO

Sección V
Disposiciones Sobre los Contratos

5.1 Condiciones Generales del Contrato

5.1.1 Validez del Contrato

El Contrato será válido cuando se realice conforme al ordenamiento jurídico y cuando el acto definitivo de Adjudicación y la constitución de la Garantía de Fiel Cumplimiento de Contrato sean cumplidos.

5.1.2 Garantía de Fiel Cumplimiento de Contrato

La Garantía de Fiel Cumplimiento de Contrato corresponderá a **Presentación de Garantía, Póliza de Fianza o Garantía Bancaria**. La vigencia de la garantía será de **un (1) año renovable,** contados a partir de la constitución de la misma hasta el fiel cumplimiento del contrato.

5.1.3 Perfeccionamiento del Contrato

Para su perfeccionamiento deberán seguirse los procedimientos de contrataciones vigentes, cumpliendo con todas y cada una de sus disposiciones y el mismo deberá ajustarse al modelo que se adjunte al presente Pliego de Condiciones Específicas, conforme al modelo estándar el Sistema Nacional de Compras y Contrataciones Públicas.

5.1.4 Plazo para la Suscripción del Contrato

Los Contratos deberán celebrarse en el plazo que se indique en el presente Pliego de Condiciones Específicas; no obstante a ello, deberán suscribirse en un plazo no mayor de **veinte (20) días hábiles**, contados a partir de la fecha de Notificación de la Adjudicación.

5.1.5 Incumplimiento del Contrato

Se considerará incumplimiento del Contrato:

a. La mora del Proveedor en la entrega de los Bienes.

b. La falta de calidad de los Bienes y Servicios conexos suministrados.

c. El Suministro de menos unidades de las solicitadas, no aceptándose partidas incompletas para los adjudicatarios en primer lugar.

5.1.6 Efectos del Incumplimiento

El incumplimiento del Contrato por parte del Proveedor determinará su finalización y supondrá para el mismo la ejecución de la Garantía Bancaria de Fiel Cumplimiento del Contrato, procediéndose a contratar al Adjudicatario que haya quedado en el segundo lugar.

En los casos en que el incumplimiento del Proveedor constituya falta de calidad de los Bienes y Servicios conexos entregados o causare un daño o perjuicio a la institución, o a terceros, la Entidad Contratante podrá solicitar a la Dirección General de Contrataciones Pública, en su calidad de Órgano Rector del Sistema, su inhabilitación temporal o definitiva, dependiendo de la gravedad de la falta.

5.1.7 Ampliación o Reducción de la Contratación

La Entidad Contratante no podrá producir modificación alguna de las cantidades previstas en el Pliego de Condiciones Específicas.

5.1.8 Finalización del Contrato

El Contrato finalizará por vencimiento de su plazo, o por la concurrencia de alguna de las siguientes causas de resolución:

- Incumplimiento del Proveedor.
- Incursión sobrevenida del Proveedor en alguna de las causas de prohibición de contratar con la Administración Pública que establezcan las normas vigentes, en especial el Artículo 14 de la Ley No. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones.

5.1.9 Subcontratos

En ningún caso el Proveedor podrá ceder los derechos y obligaciones del Contrato a favor de un tercero, ni tampoco estará facultado para subcontratarlos sin la autorización previa y por escrito de la Entidad Contratante.

5.2 Condiciones Específicas del Contrato

5.2.1 Vigencia del Contrato

La vigencia del Contrato será de **tres (3) años** a partir de la fecha de la suscripción del mismo y hasta su fiel cumplimiento, de conformidad con el Cronograma de Entrega de Cantidades Adjudicadas, el cual formará parte integral y vinculante del mismo.

5.2.2 Inicio del Suministro

Una vez formalizado el correspondiente Contrato de Suministro entre la Entidad Contratante y el Proveedor, éste último iniciará el Suministro de los Bienes y Servicios conexos que se requieran mediante el correspondiente pedido, sustentado en el Cronograma de Entrega de Cantidades Adjudicadas, que forma parte constitutiva, obligatoria y vinculante del presente Pliego de Condiciones Específicas.

5.2.3 Modificación del Cronograma de Entrega

La Entidad Contratante, como órgano de ejecución del Contrato se reserva el derecho de modificar de manera unilateral el Cronograma de Entrega de los Bienes y Servicios conexos Adjudicados, conforme entienda oportuno a los intereses de la institución.

Si el Proveedor no suple los Bienes y Servicios conexos en el plazo requerido, se entenderá que el mismo renuncia a su Adjudicación y se procederá a declarar como Adjudicatario al que hubiese obtenido el segundo (2do.) lugar y así sucesivamente, en el orden de Adjudicación y de conformidad con el Reporte de Lugares Ocupados. De presentarse esta situación, la Entidad Contratante procederá a ejecutar la Garantía Bancaria de Fiel Cumplimiento del Contrato, como justa indemnización por los daños ocasionados.

5.2.4 Entregas Subsiguientes

Las entregas subsiguientes se harán de conformidad con el Cronograma de Entrega establecido.

Las Adjudicaciones a lugares posteriores podrán ser proporcionales, y el Adjudicatario deberá indicar su disponibilidad en un plazo de **Cuarenta y Ocho (48) horas**, contadas a partir de la recepción de la Carta de Solicitud de Disponibilidad que al efecto le será enviada.

Los documentos de despacho a los almacenes de la Entidad Contratante deberán reportarse según las especificaciones consignadas en la Orden de Compra, la cual deberá estar acorde con el Pliego de Condiciones Específicas.

PARTE 3
ENTREGA Y RECEPCIÓN

Sección VI
Recepción de los Productos

6.1 Requisitos de Entrega

Todos los Bienes y Servicios conexos adjudicados deben ser entregados conforme a las especificaciones técnicas solicitadas, así como en el lugar de entrega convenido con **el Programa de Administración Financiera Integrada (PAFI) del Ministerio de Hacienda**, siempre con previa coordinación con el responsable de recibir la mercancía y con el encargado del almacén con fines de dar entrada a los Bienes y Servicios conexos entregados.

6.2 Recepción Provisional

El Encargado de Almacén y Suministro debe recibir los Bienes y Servicios conexos de manera provisional hasta tanto verifique que los mismos corresponden con las características técnicas de los bienes adjudicados.

6.3 Recepción Definitiva

Si los Bienes y Servicios conexos son recibidos CONFORME y de acuerdo a lo establecido en el presente Pliegos de Condiciones Específicas, en el Contrato u Orden de Compra, se procede a la recepción definitiva y a la entrada en Almacén para fines de inventario.

No se entenderán suministrados, ni entregados los Bienes y Servicios conexos que no hayan sido objeto de recepción definitiva.

6.4 Obligaciones del Proveedor

El Proveedor está obligado a reponer Bienes y Servicios conexos deteriorados durante su transporte o en cualquier otro momento, por cualquier causa que no sea imputable a la Entidad Contratante.

Si se estimase que los citados Bienes y Servicios conexos no son aptos para la finalidad para la cual se adquirieron, se rechazarán los mismos y se dejarán a cuenta del Proveedor, quedando la Entidad Contratante exenta de la obligación de pago y de cualquier otra obligación.

El Proveedor es el único responsable ante Entidad Contratante de cumplir con el Suministro de los renglones que les sean adjudicados, en las condiciones establecidas en los presente Pliegos de Condiciones Específicas. El Proveedor responderá de todos los daños y perjuicios causados a la Entidad Contratante y/o entidades destinatarias y/o frente a terceros derivados del proceso contractual.

Sección VII
Formularios

7.1 Formularios Tipo

El Oferente/Proponente deberá presentar sus Ofertas de conformidad con los Formularios determinados en el presente Pliego de Condiciones Específicas, **los cuales se anexan como parte integral del mismo.**

7.2 Anexos

1. Modelo de Contrato de Ejecución de Servicios **(SNCC.C.024)**
2. Presentación Formulario de Oferta Económica **(SNCC.F.033)**
3. Presentación de Oferta **(SNCC.F.034)**
4. Garantía de Cumplimiento de Contrato **(SNCC.D.038)**, si procede.
5. Formulario de Información sobre el Oferente **(SNCC.F.042)**
6. Currículo del Personal Profesional propuesto **(SNCC.D.045)**, si procede.
7. Experiencia profesional del Personal Principal **(SNCC.D.048)**, si procede.
8. Experiencia como Contratista **(SNCC.D.049)**

Nota: debe enviarse un correo solicitando los formularios anexos (Correo electrónico: yefernandez@hacienda.gov.do,).